



CUR CHUIGE CÉIM AR CHÉIM FAOI CONAS CSIRT A CHUR AR BUN

Innéacs

1. Achoimre Bhainistíochta	2
2. Fógra dlíthiúil	2
3. Buíochas	2
4. Réamhrá	3
4.1 AN LUCHT ÉISTEACHTA A BHFUILTEAR AG DÍRÍÚ AIR	4
4.2 CONAS AN DOICIMÉAD SEO A ÚSÁID	4
4.3 NÓSMHAIREACHTAÍ A ÚSÁIDTEAR SA DOICIMÉAD SEO	5
5. Straitéis fhoriomlán maidir le CSIRT a phleanáil agus a chur ar bun	6
5.1 CÉARD É CSIRT?	6
5.2 NA SEIRBHÍÍ A D'FHÉADFADH CSIRT A SHOLÁTHAR	10
5.3 ANAILS AR AN GCLIANTACHT AGUS AN RÁITEAS MISIN	12
6. An Plean Gnó a Fhorbairt	18
6.1 AN MÚNLA AIRGEADAIS A SHAINMHÍNIÚ	18
6.2 AN STRUCHTÚR EAGRÚCHÁIN A SHAINMHÍNIÚ	20
6.3 AN FHOIREANN CHEART A EARCÚ	24
6.4 ÚSÁID AGUS TREALAMH NA HOIFIGE	26
6.5 POLASAÍ SLÁNDÁLA FAISNÉISE A FHORBAIRT	28
6.6 COMHOIBRIÚ A LORG IDIR CSIRT-ANNA EILE AGUS TIONSCNAIMH IONCHASACHA NÁISIÚNTA	29
7. An Plean Gnó a Chur Chun Cinn	32
7.1 CUR SÍOS AR PHLEANANNA GNÓ AGUS AR THRUICIR BHAINISTÍOCHTA	34
8. Samplaí de nósanna imeachta oibríochta agus teicniúla (sreabhadh oibre)	37
8.1 BONN SUITEÁLA NA CLIANTACHTA A MHEASÚNÚ	38
8.2 FOLÁIRIMH, RABHAIDH AGUS FÓGAIRTÍ A GHINIÚINT	39
8.3 LÁIMHSEÁIL TEAGMHAS A CHUR I NGNÍOMH	46
8.4 SAMPLA D'AMCHLÁR FREAGARTHA	52
8.5 UIRLISIÚ CSIRT ATÁ AR FÁIL	53
9. Oiliúint CSIRT	55
9.1 TRANSITS	55
9.2 CERT/CC	56
10. Ceacht: ábhar comhairleach a ullmhú	58
11. Conclúid	63
12. Cur síos ar Phlean Tionscadail	64
AGUISÍN	66
A.1 TUILLEADH ÁBHAIR LÉITHEOIREACHTA	66
A.2 SEIRBHÍÍ CSIRT	67
A.3 NA SAMPLAÍ	77
A.4 ÁBHAR SAMPLACH AS CÚRSAÍ CSIRT	81

1. Achoimre Bhainistíochta

Sa doiciméad seo, déantar cur síos ar an bpróiseas a bhaineann le Foireann Slándála Ríomhaireachta agus Freagartha Teagmhais (CSIRT) a chur ar bun í thaobh na bpeirspictíochtaí iomchuí go léir, mar shampla bainistíocht ghnó, bainistíocht phróiseas agus peirspictíocht theicniúil. Tríd an doiciméad seo, déantar dhá cheann de na torthaí inseachadta a thuairiscítear i gClár Oibre ENISA 2006, caibidil 5.1 a chur i bhfeidhm:

- An doiciméad seo: *Tuarascáil i scríbhinn ar chur chuige céim ar chéim faoi conas CERT nó saoráidí comhchosúla a chur ar bun, agus samplaí san áireamh (CERT-D1)*
- Caibidil 12 agus comhaid sheachtracha: *Sliocht as léarscáil bhóthair i bhfoirm mhionsonraithe trína n-éascaítear an léarscáil bhóthair a chur i bhfeidhm go praiticiúil. (CERT-D2)*

2. Fógra dlíthiúil

Ní mór duit a thabhairt do d'aire gurb ionann an foilseachán seo agus tuairimí agus léirithe na n-údar agus na n-eagarthóirí, mura luaitear a mhalairt. Ní ceart an foilseachán seo a fhorléiriú mar ghníomh de chuid ENISA nó de chuid chomhlachtaí ENISA mura nglactar é de bhun Rialachán ENISA (CE) Uimh 460/2004. Ní gá go léiríonn an foilseachán seo an staid is nua-aimseartha agus d'fhéadfadh sé tarlú go ndéanfar é a uasdátú ó am go ham.

Déantar foinsí tríú páirtí a lua de réir mar is cuí. Níl ENISA freagrach as ábhar de chuid foinsí seachtracha lena n-áirítear láithreáin sheachtracha gréasáin dá dtagraítear san fhoilseachán seo.

Tá an foilseachán seo beartaithe chun críoch oideachais agus faisnéise amháin. Níl ENISA ná aon duine atá ag gníomhú thar a cheann freagrach as aon úsáid a bhainfeá as an bhfaisnéis atá san fhoilseachán seo.

Gach ceart ar cosnamh. Ní fhéadfar aon chuid den fhoilseachán seo a atáirgeadh, a stóráil i gcóras aisghabhála nó a thraseoladh in aon fhoirm nó ar aon mhodh, cibé acu leictreonach nó meicniúil, a fhótachóipeáil, a thaifeadadh, nó a úsáid ar aon slí eile gan cead a fháil roimh ré ó ENISA, nó ní fhéadfar é a úsáid ach amháin mar a cheadaítear go sainráite le Dlí nó faoi théarmaí arna gcomhaontú leis na heagraíochtaí ceart cuí. Ní mór admháil a thabhairt i leith na foinse gach tráth. Is féidir fiosruithe maidir le hatáirgeadh a chur chuig an seoladh teagmhála atá luaite san fhoilseachán seo.

© An Ghníomhaireacht Eorpach Slándála Gréasáin agus Faisnéise (ENISA), 2006

3. Buíochas

Is mian le ENISA buíochas a ghabháil leis na hinstiúidí agus leis na daoine go léir a bhí bainteach leis an doiciméad seo. Déantar buíochas ar leith a ghabháil leis seo a leanas:

- Henk Bronk, a ghníomhaigh mar shainchomhairleoir agus a d'ullmhaigh an chéad leagan den doiciméad seo

- An CERT/CC agus go háirithe foireann forbartha CSIRT, a thug ábhar an-úsáideach mar aon leis an ábhar samplach cúrsa san iarscríbhinn.
- GovCERT.NL as *CERT-i-mbosca* a sholáthar
- Foireann TRANSITS a thug an t-ábhar samplach cúrsa san iarscríbhinn.
- Comhghleacaithe as an rannóg Bheartas Slándála sa Roinn Theicniúil a thug cabhair maidir le caibidil 6.6
- An líon as cuimse daoine a d'athbhreithnigh an doiciméad

4. Réamhrá

Tá gréasáin chumarsáide agus córais fhaisnéise tar éis teacht chun bheith ina ngné riachtanach den fhorbairt eacnamaíochta agus den fhorbairt shóisialta. Tá an ríomhaireacht agus gréasánú ag teacht chun bheith ina bhfóntais uileláithreacha anois sa tslí chéanna ina bhfuil an tréith sin ag leictreachas agus ag uisce.

Dá bhrí sin, is ábhar méadaitheach inní don tsochaí é slándáil gréasán cumarsáide agus córas faisnéise agus infhaighteacht na nithe sin. Éiríonn an t-ábhar inní sin as an bpríacal go mbeidh fadhbanna ann maidir le córais thábhachtacha faisnéise, ar fadhbanna iad a éiríonn mar gheall ar chastacht chórais, ar thionóiscí, ar bhotúin agus ar ionsaithe ar bhonneagair fhisiciúla trína soláthraítear seirbhísí atá rí-thábhachtach i gcomhthéacs leas shaoránaigh an AE.

Ar an 10 Márta 2004, cuireadh Gníomhaireacht Eorpach Slándála Gréasáin agus Faisnéise (ENISA) ar bun¹. Ba é an cuspóir a bhí aige ná a chinntiú go mbeadh ardleibhéal slándála gréasáin agus faisnéise ann laistigh den chomhphobal agus forbairt a dhéanamh ar chultúr slándála gréasáin agus faisnéise ar mhaithe le saoránaigh, custaiméirí, fiontair agus eagraíochtaí earnála poiblí laistigh den Aontas Eorpach, agus ar an dóigh sin cabhair a thabhairt maidir le feidhmiú réidh an mhargaidh inmheánaigh.

Le tamall de bhlianta anuas, tá roinnt comhphobal slándála san Eoraip, ar nós CERT/CSIRT-anna, Foirne Drochúsáide agus WARP-anna, tar éis comhoibriú lena chéile ar mhaithe le hídirlíon níos daingne. Tá se beartaithe ag ENISA tacú leis na comhphobail sin ina gcuid iarrachtaí trí fhaisneis a sholáthar faoi bhearta chun leibhéal cuí cáilíochta seirbhíse a áirithiú. Ina theannta sin, tá sé beartaithe ag ENISA feabhas a chur ar a chumas chun comhairle a thabhairt do na ballstait den AE agus do na comhlachtaí den AE lena mbaineann maidir le saincheisteanna faoi chlúdach seirbhísí cuí slándála a sholáthar do ghrúpaí sonracha úsáideoirí IT. Dá bhrí sin, trí leas a bhaint as cinntí an Ghrúpa Oibre ad hoc, Comhar agus Tacaíocht CERT, a bunaíodh sa bhliain 2005, déileálfaidh an Grúpa Oibre nua sin le saincheisteanna a bhaineann le seirbhísí dóthanacha slándála ("seirbhísí CERT") a sholáthar d'úsáideoirí sonracha (nó d'eamálacha sonracha nó do ghrúpaí sonracha úsáideoirí).

Tacaíonn ENISA le bunú CSIRT-anna nua tríd an tuarascáil seo de chuid ENISA "Cur

¹ Rialachán (EC) Uimh 460/2004 an 10 Márta 2004 lena mbunaítear an Gníomhaireacht Eorpach Slándála Gréasáin agus Faisnéise. Is é atá in "Gníomhaireacht de chuid an Chomhphobail Eorpach" ná comhlacht arna chur ar bun ag an AE chun cúram sonrach teicniúil, eolaíochta nó bainistíochta ar leith a chomhall de réir "an fearann Comhphobail" ("an chéad cholún") den AE

chuige céim ar chéim faoi conas CSIRT a chur ar bun mar aon le seicliosta forlíontach”, ar tuarascáil í a chuideoidh leat do CSIRT fein a bhunú.

4.1 An lucht éisteachta a bhfuiltear ag díriú air

Is é an príomhlucht éisteachta atá i gceist le haghaidh na tuarascála seo ná institiúidí rialtais agus institiúidí eile a chinneann CSIRT a chur ar bun chun a mbuneagar IT féin nó bonneagar IT páirtithe eile a bhaineann leo a chosaint.

4.2 Conas an doiciméad seo a úsáid

Sa doiciméad seo, soláthrófar faisnéis faoi céard é CSIRT, cé na seirbhísí is féidir leis a sholáthar agus cad iad na bearta riachtanacha chun dul i mbun oibre. Is ceart go dtabharfadh an meid sin forléargas maith pragmatach ar an cur chuige, ar an struchtúr agus ar an ábhar atá i gceist maidir le CSIRT a chur ar bun.

Caibidil 4 “Réamhrá”

Réamhrá faoin tuarascáil seo

Caibidil 5 “Straitéis fhoriomlán maidir le CSIRT a phleanáil agus a chur ar bun”

Sa chéad roinn, tugtar cur síos ar céard é CSIRT. Soláthrófar faisnéis inti freisin faoi na timpeallachtaí éagsúla inar féidir leas a bhaint as CSIRT-anna agus faoi na seirbhísí is féidir a sholáthar dá mbarr.

Caibidil 6 “An Plean Gnó a Fhorbairt”

Sa chaibidil seo, déantar cur síos ar an gcur chuige bainistíochta gní a ghabhann le CSIRT a chur ar bun.

Caibidil 7 “An Plean Gnó a Chur Chun Cinn”

Sa chaibidil seo, déileáiltear leis an gcás gnó agus le nithe a bhaineann le maoiniú.

Caibidil 8 “Samplaí de nósanna imeachta de chineál oibríochtúil agus teicniúil”

Sa chaibidil seo, déantar cur síos ar an nós imeachta a bhaineann le faisnéis a fháil agus an fhaisnéis sin a aistriú ina fheasachán slándála. Sa chaibidil seo freisin, soláthraítear cur síos ar shreabhadh oibre i dtaca le láimhseáil teagmhas.

Caibidil 9 “Oiliúint CSIRT”

Sa chaibidil seo, tugtar achoimre ar an oiliúint CSIRT atá ar fáil. Mar léiriú air sin, tá ábhar samplach cúrsa ar fáil san aguisín.

Caibidil 10 “Ceacht: ábhar comhairleach a ullmhú”

Sa chaibidil seo, faightear ceacht i dtaobh conas ceann de bhunseirbhísí (nó lárseirbhísí) CSIRT a chur i gcrích: feasachán slándála (nó ábhar comhairleach) a ullmhú.

Caibidil 12 “Cur Síos ar an bPlean Tionscadail”

Sa chaibidil seo, déantar tagairt don phlean tionscadail forlíontach (seicliosta) a sholáthraítear in éineacht leis an treoir seo. Is é is aidhm don phlean seo ná a bheith ina uirlis shimplí i gcomhair chur i bhfeidhm na treorach seo.

4.3 Nósmhaireachtaí a úsáidtear sa doiciméad seo

Chun treoir a chur ar fáil don léitheoir, tá achoimre ann ag tús gach caibidle ar achoimre é ar na bearta atá déanta go dtí seo maidir le CSIRT a chur ar bun. Leagtar amach na hachoirí sin i mboscaí den chineál seo a leanas:

Tá an chéad bheart déanta againn

Ag deireadh gach caibidle, gheofar sampla praiticiúil ar na bearta a phléitear. Sa doiciméad seo, is é a bheidh sa “CSIRT Samhailteach” ná CSIRT beag neamhspleách do chuideachta nó d’institiúid bheag neamhspleách. Tá achoimre le fáil san aguisín.

CSIRT samhailteach

5. Straitéis fhoriomlán maidir le CSIRT a phleanáil agus a chur ar bun

Le go gcuirfead tús rathúil leis an bpróiseas a ghabhann le CSIRT a chur ar bun, tá se tábhachtach go mbeadh fíis shoiléir ann faoi na seirbhísí ionchasacha is feidir leis an bhfoireann a sholáthar dá custaiméirí ar a dtugtar ‘cliain’ de réir “caint CSIRT”. Dá bhrí sin, chun na seirbhísí cuí a sholáthar go trathúil agus de reir caighdeáin chuí, is gá tuiscint a bheith ann ar riachtanais na gcliain.

5.1 Céard é CSIRT?

Ciallaíonn CSIRT Foireann Freagartha Teagmhais Slándála Ríomhaire. I Stáit Aontaithe Mheiriceá is mó a úsáidtear an téarma CSIRT i gcomhair an téarma chosanta CERT atá cláraithe i Stáit Aontaithe Mheiriceá ag an CERT Coordination Center (CERT/CC).

Tá giorrúcháin éagsúla ann a úsáidtear le haghaidh an chineáil chéanna foirne:

- CERT nó CERT/CC (Foireann Freagartha Éigeandála Ríomhaire/Foireann Chomhordúcháin)
- CSIRT (Foireann Freagartha Teagmhais Slándála Ríomhaire)
- IRT (Foireann Freagartha Teagmhais)
- CIRT (Foireann Freagartha Teagmhais Ríomhaire)
- SERT (Foireann Freagartha Éigeandála Slándála)

Le linn bhlianta deiridh na 1980-idí a tharla an chéad ráig mór, i dtaca le worm de, sa bhonneagar domhanda IT. Ba é an t-ainm a bhí ar an worm ná Morris²; leath sé go mear agus, le fírinne, fabhtaíodh líon mór córas IT ar fud an domhain dá bharr.

B’ionann an teagmhas sin agus glao aláirim: d’éirigh daoine eolach go tobann ar an ngá méadaithe le comhoibriú agus comhordú idir riarthóirí córas agus bainisteoirí IT chun déileáil le cásanna den sórt seo. Ó tharla go raibh am an-tábhachtach, b’éigean cur chuige níos eagraithe agus níos struchtúrtha a bhunú chun teagmhais slándála ríomhaire a láimhseáil. Agus, dá bhrí sin, cúpla lá tar éis “teagmhas Morris” bhunaigh an Ghníomhaireacht Cosanta um Thionscadail Ard-Taighde (DARPA) an chéad CSIRT riamh: an CERT Coordination Center (CERT/CC)³, a bhí suite in Ollscoil Carnegie Mellon in Pittsburgh (Pennsylvania).

Ba ghearr gur glacadh an múnla sin laistigh den Eoraip, agus sa bhliain 1992 rinne an solathróir Acadúil Dúitseach SURFnet tús a chur leis an gcéad CSIRT san Eoraip, ar a dtugtar SURFnet-CERT⁴. Lean cuid mhór foirne an sampla sin agus faoi láthair tá níos mó ná 100 foireann is eol a bheith lonnaithe san Eoraip liostaithe i ndoiciméad de chuid ENISA dar teideal *Fardal ghníomhaíochtaí CERT san Eoraip*⁵.

Thar na blianta, leathnaigh CERT-anna a gcumais chun teacht chun bheith ina

² Tá tuilleadh faisnéise faoin Morris Worm le fáil ag http://en.wikipedia.org/wiki/Morris_worm

³ CERT-CC, <http://www.cert.org>

⁴ SURFnet-CERT: <http://cert.surfnet.nl/>

⁵ Fardal ENISA http://www.enisa.europa.eu/cert_inventory/

solathróirí seirbhíse iomláine slándála seachas ina bhfórsa freagartha agus áirítear seirbhísí den chineál seo a leanas ina gcuid seirbhísí: seirbhísí coisctheacha ar nós foláireamh, ábhar comhairleach maidir le slándáil, oiliúint agus seirbhísí bainistíochta slándála. Roimh i bhfad, measadh nár leor an téarma “CERT”. Dá thoradh sin, bunaíodh an téarma nua “CSIRT” ag deireadh bhlianta na 1990-idí. Faoi láthair, tá an dá thearma (CERT and CSIRT) á n-úsáid go comhchiallach ach is é CSIRT an téarma is cruinne díobh.

5.1.1 An téarma *Cliantacht*

As seo amach (i gcomhphobail CSIRT) déanfar an téarma seanbhunaithe ‘cliantacht’ a úsáid chun tagairt a dhéanamh do bhonn cliant CSIRT. Tabharfar ‘cliant’ ar chustaiméir aonair agus tabharfar ‘cliaint’ ar ghrúpa custaiméirí.

5.1.2 Sainmhíniú ar CSIRT

Is é atá in CSIRT ná foireann saineolaithe slándála IT arb é an príomhghnó atá acu ná déileáil le teagmhais slándála ríomhaire. Soláthraíonn sé na seirbhísí riachtanacha chun teagmhais den sórt sin a láimhseáil agus chun tacú lena gcliaint maidir le teacht slán tar éis sárúithe.

Chun priacail a mhaolú agus an líon freagairtí a íoslaghdú, soláthraíonn an chuid is mó CSIRT-anna seirbhísí coisctheacha agus seirbhísí oideachais dá gcliantacht freisin. Eisíonn siad ábhar comhairleach maidir le leochaileachtaí sna bogearraí agus sna cruaearraí atá in úsáid agus, chomh maith leis sin, déanann siad úsáideoirí a chur ar an eolas faoi dhúshaothú agus faoi víris a bheireann buntaiste ar fhabhtanna den sórt sin. Dá bhrí sin, bíonn na cliaint in ann a gcórais a phaisteáil agus a uasdátú go tapa. Féach caibidil 5.2 *Seirbhísí ionchasacha* chun liosta iomlán de na seirbhísí ionchasacha a fháil.

5.1.3 Na tairbhí a ghabhann le CSIRT a bheith agat

Nuair atá sainfhoireann slándála IT ann is cabhair í d’eagraíocht i dtaca le mórtheagmhais a mhaolú agus a chosc agus is cabhair í i dtaca lena sócmhainní luachmhara a chosaint.

Seo a leanas tairbhí ionchasacha eile:

- Comhordú lárnaithe a bheith ann le haghaidh saincheistanna slándála IT laistigh d’eagraíocht (Pointe Teagmhála, PoC).
- Sainláimhseáil lárnaithe i gcomhair theagmhais IT agus déileáil leo go sainiúil agus go látnach.
- Oilteacht a bheith ar an láthair chun tacú agus cabhrú le húsáideoirí teacht slán tar éis teagmhais slándála.
- Déileáil le saincheistanna dlíthiúla agus fianaise a chaomhnú i gcás caingean dlí a bheith ann.
- Forbairtí i réimse na slándála a rianú.
- Comhoibriú a spreagadh laistigh den chliantacht maidir le slándáil IT (cur le feasacht).

CSIRT samhailteach (beart 0)**Tuiscint a fháil ar céard é CSIRT:**

Ní mór don CSIRT samplach fónamh d'institiúid mheánmheide ina bhfuil 200 fostaí. Tá a roinn IT féin ag an institiúid mar aon le dhá oifig chraoibhe sa tír chéanna. Tá ról tábhachtach ag IT sa chuideachta mar go n-úsáidtear é le haghaidh cumarsáide inmheánaí, le haghaidh gréasáin sonraí agus le haghaidh ríomhghnó 24x7. Tá a gréasán féin ag an institiúid agus diúscaíonn sí ceangal iomarcach leis an idirlíon trí dhá ISP éagsúla.

5.1.4 Cur síos ar na cineálacha éagsúla timpeallachtaí CSIRT

Tá an chéad bheart déanta againn

1. Tuiscint a fháil ar céard é CSIRT agus cé na tairbhí a d'fhéadfadh a bheith ann dá bharr.

>> Is é an chéad chéim eile ná freagra a thabhairt ar an gceist seo a leanas: "Cén earnáil a soláthrófar seirbhísí CSIRT di?"

Nuair atá tús á chur le CSIRT (dála aon ghnó eile) tá sé an-tábhachtach tuairim shoiléir a bheith ann go luath sa phróiseas faoi cé hiad na cliaint agus cén cineál timpeallacht a mbeidh seirbhísí CSIRT á soláthar di. Déantar idirdhealú anois idir 'na hearnálacha' seo a leanas:

- CSIRT Earnála Acadúla
- CSIRT Tráchtála
- CSIRT Earnáil CIP/CIIP
- CSIRT Earnála Rialtais
- CSIRT Inmheánach
- CSIRT Earnála Míleata
- CSIRT Náisiúnta
- CSIRT Earnála Fiontar Beag & Meánmheide (SME)
- CSIRT Díoltóirí

CSIRT Earnála Acadúla*Fócas*

Soláthraíonn CSIRT earnála acadúla seirbhísí CSIRT d'institiúidí acadúla agus oideachais, ar nós ollscoileanna nó saoráidí taighde agus dá dtimpeallachtaí idirlín campais.

Cliaint

De ghnáth, is é atá i gcliaint an chineáil seo CSIRT ná foireann agus mic léinn ollscoileanna.

CSIRT Tráchtála*Fócas*

Soláthraíonn CSIRT tráchtála seirbhísí CSIRT ar bhonn tráchtála dá gcliaint. I gcás ISP,

soláthraíonn an CSIRT seirbhísí droch-úsáide do chustaiméirí deiridh (Dialligh Isteach, ADSL) agus seirbhísí CSIRT dá gcustaiméirí gairmiúla.

Cliaint

De ghnáth, soláthraíonn CSIRT-anna a gcuid seirbhísí do chliaint a íocann astu.

CSIRT Earnáil CIP/CIIP

Fócas

Díríonn CSIRT-anna san earnáil seo go príomha ar Chosaint Faisnéise Fíorthábhachtaí agus/nó ar chosaint Faisnéise Fíorthábhachtaí agus Bonneagair Fhíorthábhachtaigh. Sa chuid is mó cásanna, comhoibríonn an CSIRT sainiúil seo go dlúth le roinn CIIP Rialtais. Cuimsíonn sé na hearnálacha fíorthábhachtacha IT go léir sa tír agus cosnaíonn sé saoránaigh na tíre sin.

Cliaint

Rialtas; gnóthaí fíorthábhachtacha IT; saoránaigh

CSIRT Earnála Rialtais

Fócas

Soláthraíonn CSIRT rialtais seirbhísí do ghníomhaireachtaí rialtais agus, i roinnt tíortha, do na saoránaigh.

Cliaint

Rialtais agus gníomhaireachtaí a bhfuil baint acu le rialtais; i roinnt tíortha, soláthraítear seirbhísí foláirimh do na saoránaigh freisin (mar shampla, sa Bheilg, san Ungáir, san Ísiltír, sa Ríocht Aontaithe nó sa Ghearmáin).

CSIRT Inmheánach

Fócas

Soláthraíonn CSIRT inmheánach seirbhísí dá eagraíocht óstach agus don eagraíocht sin amháin. Is cur síos é sin ar an fheidhm seachas ar earnáil. Mar shampla, tá a gcuid CSIRT-anna féin ag a lán eagraíochtaí teileachumarsáide agus banc. De ghnáth, ní chothabhálann siad láithreán gréasáin don phobal.

Cliaint

Foireann inmheánach agus roinn IT na heagraíochta óstaí.

CSIRT Earnála Míleata

Fócas

Soláthraíonn CSIRT de chuid na hearnála seo seirbhísí d'eagraíochtaí míleata ar a bhfuil freagrachtaí maidir le bonneagar IT atá ag teastáil chun críoch cosanta.

Cliaint

Foireann de chuid institiúidí míleata nó de cuid eintiteas a bhfuil dlúthbhaint acu le h-institiúidí míleata, mar shampla an Roinn Cosanta.

CSIRT Náisiúnta

Fócas

CSIRT lena ngabhann fócas náisiúnta agus a meastar ina leith gur pointe teagmhála

slándála i gcomhair tíre. I roinnt cásanna, gníomhaíonn an CSIRT rialtais mar PoC náisiúnta freisin (ar nós UNIRAS sa Ríocht Aontaithe).

Cliaint

De ghnáth, ní bhíonn cliaint dhíreacha ag an gcineál seo CSIRT, mar nach mbíonn ach ról idirghabhálach ag an CSIRT náisiúnta i dtaca leis an tír lena mbaineann ina hiomláine.

CSIRT Earnála Fiontar Beag & Meánmhéide (SME)

Fócas

CSIRT féineagraithe a sholáthraíonn a sheirbhísí dá chraobh ghnó féin nó do ghrúpa úsáideoirí eile den tsamhail chéanna.

Cliaint

D'fhéadfadh sé gur é atá i gcliain na CSIRT-anna seo ná SME-anna agus a bhfoireann, nó grúpaí speisialta ar nós "Cumann Bailte agus Bardas" de chuid tíre.

CSIRT Díoltóirí

Fócas

Díríonn CSIRT díoltóirí ar thacaíocht a thabhairt i leith táirgí a bhaineann go sonrach le díoltóirí. Is é is aidhm dó de dhnáth ná reitigh a aimsiú agus a fhorbairt chun deireadh a chur le laigí agus maolú a dhéanamh ar na hiarmhairtí diúltacha ionchasacha a d'fhéadfadh a bheith ann de thoradh lochtanna.

Cliaint

Úinéirí táirgí

De réir na tuairisce a thugtar sa mhír a bhaineann le CSIRT-anna náisiúnta, d'fhéadfadh sé tarlú go bhfónann foireann amhain do níos mó ná earnáil amháin. Bíonn tionchar aige sin ar an anailís a dhéantar ar an gcliantacht agus ar a riachtanais.

CSIRT samhailteach (beart 1)

An chéim thosaigh

Ag an gcéim thosaigh, déantar an CSIRT nua a phleanáil mar CSIRT Inmheánach agus soláthraítear a chuid seirbhísí don chuideachta óstach, don roinn IT áitiúil agus don fhoireann. Déanann sé tacaíocht agus comhordú a sholáthar freisin in oifigí craoibhe éagsúla maidir le láimhseáil teagmhas a bhaineann le slándáil.

5.2 Na seirbhísí a d'fhéadfadh CSIRT a sholáthar

Tá an chéad dá bheart déanta againn

1. Tuiscint a fháil ar céard é CSIRT agus cé na tairbhí a d'fhéadfadh a bheith ann dá bharr.
2. Cén earnáil a soláthróidh an fhoireann nua a cuid seirbhísí di?

>> Is é an chéad chéim eile ná freagra a thabhairt ar an gceist seo a leanas: *cad iad na seirbhísí a sholáthrófar do na cliaint.*

Tá a lán seirbhísí ann atá CSIRT ina ann a sholáthar, ach go dtí seo níl aon CSIRT amháin ann a sholáthraíonn gach ceann de na seirbhísí sin. Dá bhrí sin, is cinneadh thar a bheith tábhachtach an cinneadh maidir le roghnú na sraithe cuí seirbhísí. Anseo thíos, gheofar forléargas gairid ar na seirbhísí CSIRT go léir atá ann de réir mar atá leagtha amach in “Handbook for CSIRTs” arna fhoilsiú ag CERT/CC⁶.

<u>Seirbhísí Freagartha</u>	<u>Seirbhísí Gníomhaíocha</u>	<u>Láimhseáil Déantán</u>
• <u>Foláirimh agus Rabhaidh</u> • <u>Láimhseáil Teagmhas</u> • <u>Anailís Teagmhas</u> • <u>Tacaíocht Freagartha Teagmhas</u> • <u>Comhordú Freagartha Teagmhas</u> • <u>Freagairt Teagmhas ar an láthair</u> • <u>Láimhseáil laigí</u> • <u>Anailís laigí</u> • <u>Freagairt laigí</u> • <u>Comhordú freagartha laigí</u>	• <u>Fógairtí</u> • <u>Airdeall Teicneolaíochta</u> • <u>Iniúchtaí nó Measúnachtaí Slándála</u> • <u>Cumraíocht agus Cothabháil Slándála</u> • <u>Forbairt Uirlisí Slándála</u> • <u>Seirbhísí Braite Ionraidh</u> • <u>Scaipeadh Faisnéise a Bhaineann le Slándáil</u>	• <u>Anailís déantán</u> • <u>Freagairt déantán</u> • <u>Comhordú freagartha déantán</u>
		<u>Bainistíocht Cháilíochta Slándála</u> • <u>Anailís Phriacal</u> • <u>Leanúnachas Gnó agus Teacht Slán tar éis Tubaiste</u> • <u>Comhairliúchán Slándála</u> • <u>Méadú Feasachta</u> • <u>Oideachas/Oiliúint</u> • <u>Measúnú nó Deimhniú Táirgí</u>

Fíor 1 Liosta Seirbhísí CSIRT ó CERT/CC⁷

Na seirbhísí lárnacha (arna marcáil i gcló trom): déantar idirdhealú idir seirbhísí freagartha agus seirbhísí gníomhaíocha. Is é is aidhm do sheirbhísí gníomhaíocha ná teagmhais a chosc trí fheasacht a mhéadú agus trí oiliúint agus is é is aidhm do sheirbhísí freagartha ná déileáil le teagmhais agus maolú a dhéanamh an damáiste a bhíonn ann dá mbarr.

Láimhseáil déantán: baineann sé seo le hanailís a dhéanamh ar aon chomhad nó ar aon rud a aimsítear ar chóras ar comhad nó rud é a d’fhéadfadh a bheith bainteach le gníomhartha mailíseacha, ar nós iarmhairtí víreas, worm, scripteanna, traíoch, etc. Baineann sé freisin le láimhseáil faisnéise a bhailítear agus an fhaisnéis sin a scaipeadh ar dhíoltóirí agus ar pháirtithe gaolmhara eile chun cosc a chur ar leathadh earraí dochracha ina dhiaidh sin agus chun maolú a dhéanamh ar na priacail.

Seirbhísí bainistíochta Slándála agus Cáilíochta: seirbhísí lena ngabhann aidhmeanna níos fadtréimhsí agus áirítear iontu bearta sainchomhairle agus oideachais.

Féach an aguisín chun míniú mionsonraithe a fháil ar sheirbhísí CSIRT.

⁶ Lámhleabhar CERT/CC CSIRT <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

⁷ Liosta Seirbhísí CSIRT ó CERT/CC: <http://www.cert.org/csirts/services.html>

Tá sé tábhachtach go roghnófar na seirbhísí cearta do do chliant agus déanfar tuilleadh tagairtí don chéim sin den phróiseas i gcaibidil 6.1 *An Múnla Airgeadais a Shainmhíniú*.

Cuirtear tús leis an gcuid is mó CSIRT-anna trí ‘Foláirimh agus Rabhaidh’ a scaipeadh, trí ‘Fógairtí’ a dhéanamh agus trí ‘Láimhseáil Teagmhas’ a sholáthar dá gcliaint. De ghnáth, tugann na seirbhísí lárnacha sin luach maith don chliantacht i dtaca le próifíl agus aire de, agus, le fírinne, meastar gurb ionann iad agus “luach breise”.

Dea-chleachtas is ea tosú trí grúpa beag client ‘píolóta’ a chur ar bun, trí na seirbhísí lárnacha a sholáthar ar feadh tréimhse píolóta agus trí aiseolas a iarraidh ina dhiaidh sin.

De ghnáth, soláthraíonn úsáideoirí píolóta dáiríre aiseolas maith agus tugann siad cuidiú maidir le seirbhísí saindeartha a fhorbairt.

CSIRT samhailteach (beart 2)

Na seirbhísí cearta a roghnú

Ag an gcéim thosaigh, cinntear go ndíreofar an CSIRT nua go príomha ar roinnt seirbhísí lárnacha a sholáthar do na fostaithe.

Cinntear go ndéanfar breithniú, tar éis céime píolóta, i dtaobh leathnú an bhirt seirbhísí agus i dtaobh tús a chur le roinnt ‘Seirbhísí Bainistíochta Slandála’. Déanfar an cinneadh sin de réir an aiseolais a fhaightear ó na cliant phíolóta agus i ndlúthchomhar leis an roinn Deimhnithe Cáilíochta.

5.3 Anails ar an gcliantacht agus an ráiteas misin

Tá an chéad trí bheart déanta againn:

1. Tuiscint a fháil ar céard é CSIRT agus cé na tairbhí a d’fhéadfadh a bheith ann dá bharr.
2. Cén earnáil a soláthróidh an fhoireann nua a cuid seirbhísí di?
3. Cad iad na cineálacha seirbhísí atá CSIRT in ann a sholáthar dá chliantacht.

>> Is é an chéad bheart eile ná freagra a thabhairt ar an gceist, *cén cineál cur chuige is ceart a roghnú chun tús a chur leis an CSIRT?*

Is é atá sa chéad bheart eile ná scrúdú níos doimhne a dhéanamh ar an gcliantacht agus agus is é is aidhm dó go príomha ná na bealaí cearta cumarsáide a roghnú:

- Sainmhíniú ar an gcur chuige cumarsáide a thabhairt do na cliant
- An ráiteas misin a shainmhíniú
- Plean réadúil a dhéanamh maidir le cur i bhfeidhm/maidir leis an tionscadal
- Na seirbhísí CSIRT a shainmhíniú
- An struchtúr eagrúcháin a shainmhíniú
- An polasaí Slándála Faisnéise a shainmhíniú

- An fhoireann cheart a earcú
- D'oifig CSIRT a úsáid
- Comhoibriú a iarraidh idir CSIRT-anna eile agus tionscnaimh náisiúnta ionchasacha

Déanfar cur síos níos mionsonraithe ar na bearta sin sna míreanna sin ina dhiaidh seo agus is féidir iad a úsáid mar ionchur don phlean gnó agus don phlean tionscadail.

5.3.1 An cur chuige cumarsáide i leith na cliantachta

Mar atá ráite cheana féin, tá sé an-tábhachtach eolas a bheith ann ar riachtanais na cliantachta agus straitéis chumarsáide a bheith agat féin, lena n-áirítear na bealaí cumarsáide is oiriúnaí chun faisnéis a chur in iúl dóibh.

Tá roinnt dóigheanna ann, de réir theoiric na bainistíochta, chun dul i ngleic leis an bhfadhb a bhaineann le spriocghrúpa a anailísiú. Sa doiciméad seo, déanaimid cur síos ar dhá cheann díobh: anailís SWOT agus anailís PEST.

Anailís SWOT

Is é atá in Anailís SWOT ná uirlís phleanála straitéisí a úsáidtear chun measúnú a dhéanamh ar na Láidreachtaí (**S**trengths), ar na Laigí (**W**eaknesses), ar na Deiseanna (**O**pportunities), agus ar na Bagairtí (**T**hreats) a bhaineann le tionscadal nó le gnó nó le haon staid eile nach mór cinneadh a dhéanamh ina leith. Deirtear gur chruthaigh Albert Humphrey, a bhí i gceannas ar thionscadal taighde in Ollscoil Stanford le linn bhlianta na 1960-idí agus 70-idí, é trí leas a bhaint as sonraí de chuid chuideachtaí Fortune 500.⁸

Láidreacht	Laige
Deiseanna	Bagairtí

Fíor 2 Anailís SWOT

⁸ Anailís SWOT ar Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

Anailís PEST

Uirlis thábhachtach eile is ea anailís PEST agus úsáidtear go forleathan í chun an chliantacht a anailísiú d'fhonn tuiscint a fháil ar chúinsí Polaitíochta (Political), Eacnamaíochta (Economic), Socheacnamaíochta (Socio-cultural) agus Teicneolaíochta (Technological) na timpeallachta ina bhfuil CSIRT ag oibriú. Beidh sí ina cabhair maidir le cinneadh a dhéanamh i dtaobh an bhfuil an phleanáil in oiriúint don timpeallacht i gcónaí agus is dócha go mbeidh sí ina chabhair maidir le gníomhartha a sheachaint a dhéantar ar bhonn toimhdí míchearta.

Cúinsí Polaitíochta - Saincheisteanna éiceolaíochta/timpeallachta - Reachtaíocht reatha don mhargadh baile - Reachtaíocht todhchaí - Reachtaíocht Eorpach/idirnáisiúnta - Comhlachtaí agus próisis rialála - Polasaithe Rialtais - Téarma agus athrú Rialtais - Polasaithe trádála - Maoiniú, deontais agus tionscnaimh - Brústocaireacht/brúghrúpaí sa mhargadh baile - Brúghrúpaí idirnáisiúnta	Cúinsí Eacnamaíochta - Staid an gheilleagair baile - Treochtaí sa gheilleagar baile - Geilleagair agus treochtaí thar lear - Saincheisteanna ginearálta maidir le cánachas - Cánachas a bhaineann go sonrach le tairgí/seirbhísí - Saincheisteanna maidir le séasúracht/haimsir - Timthriallta margaidh agus trádála - Gnéithe sonracha maidir le tionscal - Bealaí margaidh agus treochtaí dáiliúcháin - Spreagthóirí custaiméara/úsáideora deiridh - Rátaí úis agus malairte
Cúinsí Socheacnamaíochta - Treochtaí stíle maireachtála - Déimeagrafaíocht - Dearcadh agus tuairimí tomhaltóirí - Tuairimí na meán - Athruithe sa dlí a fhearann ar ghnéithe sóisialta - Íomhá bhranda, chuideachta, theicneolaíochta - Pátrúin cheannaigh i gcás tomhaltóirí - Faisean agus rólchuspaí - Móirmeachtaí agus mórhionchair - Rochtain agus treochtaí maidir le ceannach - Gnéithe eitneacha/reiligiúnacha - Fógraíocht agus poiblíocht	Cúinsí Teicneolaíochta - Iomaíocht maidir le forbairt teicneolaíochta - Maoiniú do thaighde - Teicneolaíochtaí gaolmhara/spleáca - Teicneolaíocht ionaid/reitigh - Aibíocht teicneolaíochta - Aibíocht agus cumas monarúcháin - Faisnéis agus cumarsáid - Meicníochtaí/teicneolaíocht maidir le ceannach ag tomhaltóirí - Reachtaíocht maidir le teicneolaíocht - Deiseanna le haghaidh nuálaíochta - Rochtain ar theicneolaíocht, ceadúnúcháin, paitinní - Saincheisteanna maidir le maoin intleachtúil

Fíor 3 Múnla anailís Pest

Is féidir cur síos mionsonraithe ar anailís PEST a fháil in Wikipedia⁹.

Tugann an dá uirlis forléargas cuimsitheach struchtúrtha i dtaibh cad iad riachtanais na gcliant. Comhlánóidh na torthaí an togra gnó agus, sa tslí sin, beidh siad ina gcabhair maidir le bunú an CSIRT.

⁹ Anailís PEST ar Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Bealaí cumarsáide

Tá sé tábhachtach ábhar ar leith a chur san áireamh san anailís, is é sin le rá, na modhanna ionchasacha maidir le cumarsáid agus dáileadh faisnéise (“Conas cumarsáid a dhéanamh leis an gcliant?”)

Más féidir, is ceart breithniú a dhéanamh i dtaobh cuairteanna pearsanta a thabhairt go rialta ar na cliaint. Tá cruthúnas ann gur fusa comhoibriú a fháil trí theagmháil dhíreach a dhéanamh le daoine. Má bhíonn an dá thaobh sásta oibriú le chéile beidh caidreamh níos oscailte ann.

De ghnáth, oibríonn CSIRT-anna sraith bealaí cumarsáidí. Bhí na bealaí seo a leanas úsáideach ar bhonn praiticiúil agus is fiú iad a bhreithniú

- Láithreán gréasáin poiblí
- Limistéar do bhaill amháin ar an láithreán gréasáin
- Foirmeacha gréasáin chun teagmhais a thuairisciú
- Liostaí seoltaí ríomhphoist
- Ríomhphost pearsanta
- Fón / Facs
- SMS
- Litreacha ‘seanfhaiseanta’ i bhfoirm páipéir
- Tuarascálacha míosúla nó tuarascálacha bliantúla

Ar leith ó leas a bhaint as ríomhphost, foirmeacha gréasáin, fón nó facs chun láimhseáil teagmhas a éascú (tuairiscí ar theagmhais a ghlacadh ón gcliantacht, comhordú a dhéanamh le foirne eile nó aiseolas agus tacaíocht a thabhairt don íospartach), foilsíonn an chuid is mó CSIRT-anna a n-ábhar comhairleach slándála ar láithreán gréasáin atá ar fáil go poiblí agus trí liostaí seoltaí ríomhphoist a úsáid.

! Más féidir, is ceart faisnéis a dháileadh ar shlí dhaingean. Mar shampla, is féidir teachtaireachtaí ríomhphoist a shíniú go digiteach ach PGP a úsáid, agus is ceart sonraí íogaire a sheoladh i bhfoirm chriptithe i gcónaí.

Chun tuilleadh faisnéise a fháil féach caibidil 8.5 *Uirlisiú CSIRT atá ar fáil*. Féach freisin caibidil 2.3 den *RFC2350*¹⁰.

CSIRT samhailteach (beart 3a)

Anailís a dhéanamh ar an gcliantacht agus ar na bealaí cuí cumarsáide

Mar thoradh ar sheisiún dianmhachnaimh le roinn daoine ardleibhéil sa lucht bainistíochta agus sa chliantacht, gineadh dóthain ionchuir le haghaidh anailís SWOT. Is é a lean as sin ná an tuairim go raibh gá leis na seirbhísí lárnacha seo a leanas:

- Foláirimh agus rabhaidh
- Láimhseáil teagmhas (anailís, tacaíocht fhreagartha agus comhordú freagartha)
- Fógairtí

¹⁰ <http://www.ietf.org/rfc/rfc2350.txt>

Ní mór a chinntiú go ndéantar an fhaisnéis a dháileadh ar shlí dhea-eagraithe ionas go sroichtear an chuid is mó den chliantacht is féidir. Dá bhrí sin, cinntar go ndéanfar foláirimh, rabhaidh agus fógairtí i bhfoirm ábhair chomhairligh slándála a fhoilsiú ar shainláithreán gréasáin agus a dháileadh trí leas a bhaint as liosta seoltaí ríomhphoist. Is féidir CSIRT a úsáid chun tuairiscí teagmhais a fháil trí ríomhphoist, le teileafón agus le facs. Tá sé beartaithe go mbeidh foirm ghréasáin aontaithe ann mar chéad bheart eile.

Féach an chéad leathanach eile a bhfuil anailís samplach SWOT air.

Láidreacht - Tá eolas eigin ann laistigh den chuideachta. - Is maith leo an plean agus ta siad toilteanach comhoibriú - Tacaíocht agus maoiniú ón mbord bainistíochta	Laige - Níl mórán cumarsaide ann idir na ranna éagsúla agus na hoifigí craoibhe. - Níl aon chomhordú ann i dtaca le teagmhais IT - Cuid mhór “ranna beaga”
Deiseanna - Sruth mór faisnéise neamhstruchtúrtha maidir le leochaileacht - Géarghá le comhordú - Laghdú ar chaillteanais mar gheall ar theagmhais - Cuid mhór bealaí oscailte i dtaca le slándáil IT - An fhoireann a oiliúint maidir le slándáil IT	Bagairtí - Níl mórán airgid ar fáil - Níl mórán daoine san fhoireann - Ardmhianta - Cultúr

Fíor 4 Anailís samplach SWOT

5.3.2 Raiteas misin

Tar éis anailís a dhéanamh ar riachtanais agus ar mhianta na cliantachta i dtaca le seirbhísí CSIRT, is ceart gur é a bheidh sa chéad bheart eile ná raiteas misin a dhréachtú.

Déantar cur síos i raiteas misin ar bhunfheidhm na heagraíochta sa tsochaí, i dtéarmaí na dtáirgí agus na seirbhísí a sholáthraíonn sí dá cliaint. Is féidir a lua go sonrach ann gurb ann don CSIRT nua mar aon lena fheidhm a chur in iúl.

Is dea-chleachtas é an raiteas misin a bheith gonta gan a bheith róghairid mar, de ghnáth, fanfaidh sé gan athrú ar feadh cúpla bliain.

Seo a leanas roinnt samplaí de ráitis misin a bhaineann le CSIRT-anna atá ag feidhmiú cheana féin:

“Soláthraíonn <Ainm an CSIRT> faisnéis agus cúnamh dá <cliaint (tabhair sainmhíniú ar do chliaint)> le linn bearta gníomhaíocha a chur i bhfeidhm chun laghdú a dhéanamh ar an bpriacal go dtarlóidh teagmhais slándála ríomhaire, mar aon le gníomhú nuair a tharlaíonn siad.”

“Tacaíocht a thabhairt do <Cliaint> maidir le cosc Teagmhas Slándála a bhaineann le IT agus gníomhú má tharlaíonn a leithéid”¹¹

Is beart tosaigh an-tábhachtach agus riachtanach é an ráiteas misin. Féach caibidil 2.1 de RFC2350¹² chun cur síos níos mionsonraithe a fháil ar an bhfaisnéis is ceart a fhoilsiú in CSIRT.

CSIRT samhailteach (beart 3b)

Tá an raiteas misin seo a leanas déanta ag lucht bainistíochta an CSIRT shamhailtigh:
“Soláthraíonn CSIRT Samhailteach faisnéis agus cúnamh d’fhoireann a chuideachta óstaí chun laghdú a dhéanamh ar na priacail go mbeidh teagmhais slándála ríomhaire ann chomh maith le gníomhú má tharlaíonn teagmhais den sórt sin.”

Sa tslí sin, cuireann an CSIRT samhailteach seo in iúl go soiléir gur CSIRT inmheanach é agus gurb é atá ina ghnó lárnach ná déileáil le saincheistean a bhaineann le slándáil IT.

¹¹ Ráiteas misin Govcert.nl: <http://www.govcert.nl>

¹² <http://www.ietf.org/rfc/rfc2350.txt>

6. An Plean Gnó a Fhorbairt

Tá na bearta seo a leanas déanta againn:

1. Tuiscint a fháil ar céard é CSIRT agus cé na tairbhí a d'fhéadfadh a bheith ann dá bharr.
2. Cén earnáil a soláthróidh an fhoireann nua a cuid seirbhísí di?
3. Cad iad na cineálacha seirbhísí atá CSIRT in ann a sholáthar dá chliantacht.
4. Anailís a dhéanamh ar an timpeallacht agus ar na cliaint
5. An ráiteas misin a shainmhíniú

>> Is é atá sa chéad bheart eile na an plean gnó a shainmhíniú

Tugann aschur na hanailíse forléargas maith duit ar riachtanais agus ar laigí (toimhdean) na cliantachta; dá bhrí sin, úsáidtear an t-aschur sin mar ionchur don chéad bheart eile.

6.1 An múnla airgeadais a shainmhíniú

Tar éis an anailís a dhéanamh, roghnaíodh roinnt seirbhísí lárnacha mar phointe tosaigh. Is é atá sa chéad bheart eile ná machnamh a dhéanamh ar an múnla airgeadais: cad iad na paraiméadair soláthair seirbhíse atá oiriúnach agus iníoctha.

Dá mbeadh dálaí foirfe ann, dhéanfaí an maoiniú a oiriúnú do riachtanais na cliantachta, ach, go réadúil, ní mór an phunainn seirbhísí is féidir a sholáthar a oiriúnú don bhuiséad atá ar fáil. Dá bhrí sin, tá sé níos réadúla tosú trí shaincheistanna airgeadaíochta a phleanáil.

6.1.1 An múnla costais

Is é atá sa dá phríomhghné a imríonn tionchar ar chostais ná an líon uaire an chloig seirbhíse agus líon (agus cáilíocht) na foirne atá le húsáid. An bhfuil gá le seirbhís freagartha agus tacaíocht theicniúil 24x7 a sholáthar nó an soláthrófar na seirbhísí sin laistigh duaire oifige amháin?

Ag brath ar an infhaighteacht atá ag teastáil agus ar an trealamh oifige (mar shampla, an féidir le daoine a bheith ag obair sa bhaile?), d'fhéadfadh tairbhe a bheith ann dá mbeadh uainchlár dualgais ar gloach nó uainchlár dualgais sceidealta ann.

Cúinse inchreidte is ea seirbhísí gníomhaíochta agus seirbhísí freagartha araon a sholáthar le linn uaire oifige. Ní sholáthrófar ach seirbhísí teoranta lasmuigh d'uaire oifige, mar shampla i gcás mórthubaistí agus mórtheagmhas agus soláthróidh duine den fhoireann atá ar gloach na seirbhísí sin.

Rogha eile is ea comhoibriú idirnáisiúnta a lorg idir foirne CSIRT eile. Tá samplaí ann cheana féin de chomhoibriú ar a dtugtar "Leanúint na Gréine". Mar shampla, bhí tairbhe ag baint le comhoibriú idir foirne Eorpacha agus Meiriceánacha agus ba mhodh fóna é chun cumais an dá thaobh a chomhroinnt. Tá cuid mhór oifigí craoibhe ag CSIRT Sun

Microsystems mar shampla agus iad suite i réigiúin éagsúla ama ar fud an domhain (ach iad ina mbaill den fhoireann CSIRT céanna) agus soláthraíonn siad seirbhísí 24x7 trí dualgais a mhalartú go síoraí ó fhoireann go fhoireann ar fud an domhain. Teorannaíonn sé sin na costais mar nach mbíonn foirne ag obair ach amháin le linn gnáthuaire oifige agus soláthraíonn siad seirbhísí don chuid den domhan “atá ina chodladh”.

Is dea-chleachtas é anailís ar leith a dhéanamh ar an ngá le seirbhísí 24x7 do gach leibhéal den chliantacht. Níl mórán céille le Foláirimh agus Rabhaidh a thabhairt i rith na hoíche i gcás nach léifidh an faighteoir é go dtí an mhaidin dár gcionn. Tá líne thanaí ann idir “gá le seirbhís” agus “seirbhís ag teastáil”, ach is cinnte go bhfearann na huaire oibre go mór ar an líon foirne agus ar na saoráidí a bhfuil gá leo, agus téann sé sin i gcion go mór ar an múnla costais.

6.1.2 An múnla ioncaim

Nuair a bhíonn an costas ar eolas, is beart maith é ina dhiaidh sin machnamh a dhéanamh ar mhúnlaí ionchasacha ioncaim: conas is féidir na seirbhísí atá beartaithe a mhaoiniú. Seo a leanas roinnt cúinsí ionchasacha is ceart a mheasúnú:

Acmhainní láithreacha a úsáid

Tá sé tairbhiúil i gcónaí measúnú a dhéanamh ar na hacmhainní atá ann cheana féin i gcodanna eile den chuideachta. An bhfuil daoine oiriúnacha ar fostú san fhoireann cheana féin (mar shampla, sa roinn IT) agus an cúlra agus an oilteacht riachtanach acu? Is dócha gur féidir socruithe a dhéanamh leis an lucht bainistíochta chun daoine den sórt sin a thabhairt ar iasacht don CSIRT le linn na céime tosaigh, nó d’fhéadfadh sé go mbeadh siad in ann tacaíocht a sholáthar don CSIRT ar bhonn ad-hoc.

Táille bhallraíochta

Ionchas eile is ea do chuid seirbhísí a dhíol leis an gcliantacht, trí tháille bhliantúil/bhallraíochta a ghearradh. D’fhéadfaí íoc as seirbhísí breise ar bhonn an leibhéil úsáide, mar shampla seirbhísí sainchomhairle nó iniúchadh slándála.

Seo a leanas cúinse eile a d’fhéadfadh a bheith ann: soláthraítear seirbhísí saor in aisce don chliantacht (inmheánach) ach d’fhéadfadh sé go mbeadh táille le híoc as seirbhísí a sholáthraítear do chustaiméirí seachtracha. Smaoineamh eile is ea feasacháin chomhairle agus faisnéise a fhoilsiú ar an láithreán gréasáin agus roinn “Baill Amháin” a chur ar fáil ina bhfaighfear faisnéis speisialta atá níos mionsonraithe nó níos saineúla.

Tá cruthúnas praiticiúil ann a léiríonn nach bhfuil ach leas teoranta ag gabháil le “Sintíús in aghaidh na seirbhíse CSIRT” i dtaca le dóthain maoinithe a sholáthar, go háirithe sa chéim tosaigh. Mar shampla, tá bunchostais sheasta ann don fhoireann agus don trealamh ar costais iad atá le híoc roimh ré. Is deacair na costais sin a íoc trí sheirbhísí CSIRT a dhíol agus ní mór anailís an-mhionsonraithe airgeadais a dhéanamh chun “an pointe cómhéite airgid” a aimsiú.

Fóirdheontas

Ionchas eile is ea breithniú a dhéanamh i dtaobh iarratas a dhéanamh ar fhóirdheontas tionscadail arna sholáthar ag an rialtas nó ag comhlacht rialtais, mar, sa lá atá inniu ann, bíonn cistí ar fáil ag tíortha le haghaidh tionscadal slándála IT. D’fhéadfadh sé gur ceart, mar phointe tosaigh, teagmháil a dhéanamh leis an Roinn Rialtais lena mbaineann.

Ar ndóigh, is féidir leasa a bhaint as meascán múnlaí ioncaim.

6.2 An struchtúr eagrúcháin a shainmhíniú

Bíonn struchtúr oiriúnach eagrúcháin CSIRT ag brath go mór ar struchtúr láithreach na heagraíochta óstaí agus na cliantachta. Bíonn sé ag brath freisin ar shaineolaithe oilte a bheith ar fáil lena bhfostú ar bhonn buan nó ar bhonn ad-hoc.

I gcás gnáth-CSIRT, sainmhínítear na ról seo a leanas laistigh den fhoireann:

Ginearálta

- Bainisteoir ginearálta

Foireann

- Bainisteoir oifige
- Cuntasóir
- Sainchomhairleoir cumarsáide
- Sainchomhairleoir dlí

Foireann Theicniúil Oibríochta

- Ceannaire na foirne teicniúla
- Teicneoirí teicniúla CSIRT, a sholáthraíonn seirbhísí CSIRT
- Taighdeoirí

Sainchomhairleoirí seachtracha

- Fostaítear iad de réir riachtanais

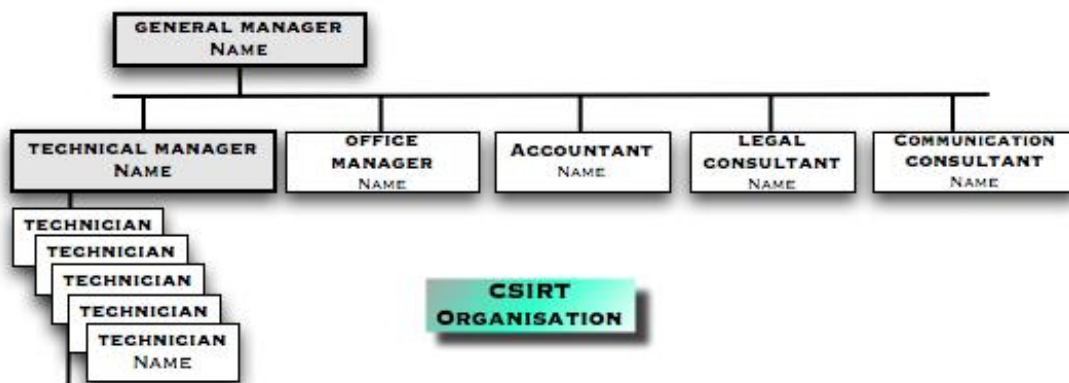
Is cabhair an-mhór é speisialtóir dlí a bheith ar an mbord go háirithe le linn na céime tosaigh den CSIRT. Cuirfidh sé sin leis an gcostas ach, i ndeireadh na dála, sábhálfar am agus fadhbanna dlí.

Ag brath ar éagsúlacht na hoilteachta atá ann sa chliantacht, agus go háirithe i gcás ardphróifíl a bheith ag an CSIRT sna meáin, tá cruthúnas ann a léiríonn go raibh sé an-fhóinteach saineolaí cumarsáide a bheith ar an bhfoireann. Is féidir leis na saineolaithe sin díriú ar shaincheistean deacra teicniúla a aistriú ina dteachtaireachtaí níos sothuigthe do na cliant nó do na comhpháirtithe sna meáin. Ina theannta sin, soláthróidh an saineolaí cumarsáide aiseolas do na saineolaithe teicniúla agus, dá bhrí sin, d'fhéadfadh sé/sí feidhmiú mar a bheadh “aistritheoir” agus “áisitheoir” ann idir an dá ghrúpa sin.

Seo a leanas roinnt samplaí de mhúnlaí eagrúcháin atá in úsáid ag CSIRT-anna atá á n-oibriú cheana féin.

6.2.1 Múnla an ghnó neamhspleách

Déantar an CSIRT a fhorbairt agus a chur i ngníomh mar eagraíocht neamhspleách lena ngabhann a lucht bainistíochta agus a fhostaithe féin.

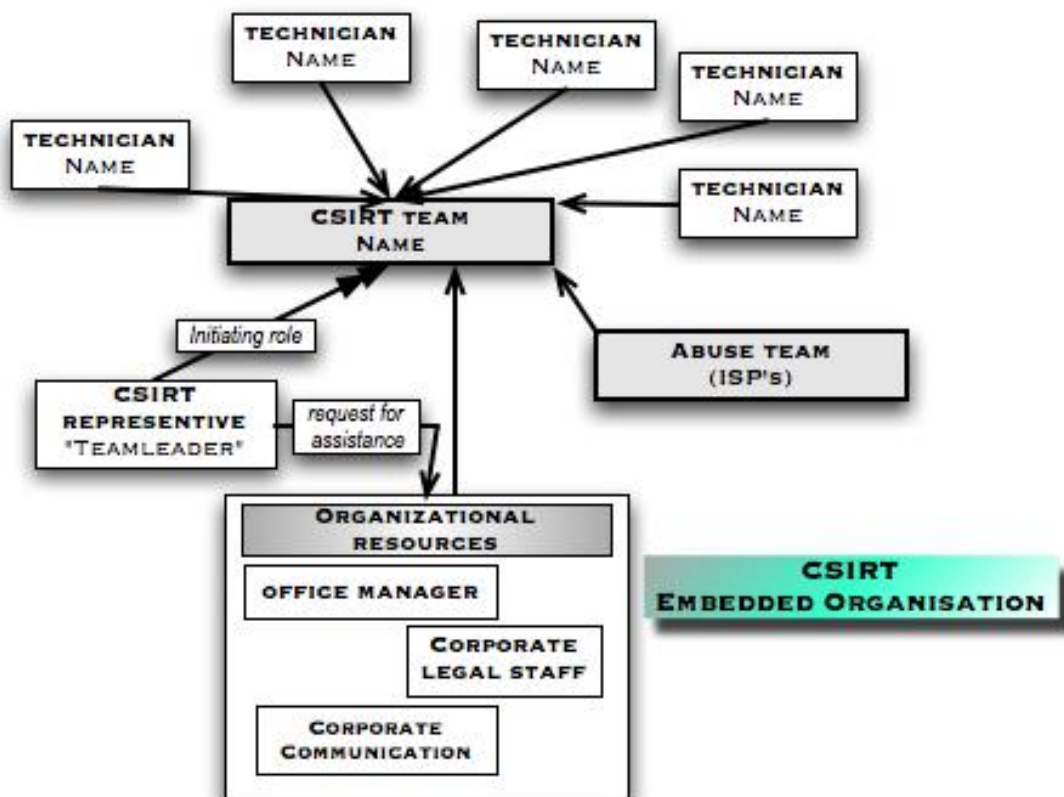


Fíor 5 Múnla an Ghnó Neamhspleách

6.2.2 An múnla leabaithe

Is féidir an múnla seo a úsáid má tá CSIRT le cur ar bun laistigh d'eagraíocht láithreach, mar shampla trí leas a bhaint as foireann láithreach IT. Bíonn ceannaire foirne i gceannas an CSIRT agus bíonn seisean/sise freagrach as na gníomhaíochtaí CSIRT. Bailíonn an ceannaire foirne na teicneoirí riachtanacha le chéile nuair atá teagmhais á réiteach nó nuair atá obair ar siúl i ndáil le gníomhaíochtaí CSIRT. Is féidir leis nó léi cúnamh a iarraidh laistigh den eagraíocht láithreach i gcás tacaíocht speisialtóra a bheith ag teastáil.

Is féidir an múnla seo a oiriúnú freisin i gcomhair staideanna sonracha de réir mar a tharlaíonn a leithéid. Sa chás sin, bíonn líon seasta Fostaithe Coibhéiseacha Lánaimseartha (FTE) ar fáil. Mar shampla, is cinnte gurb ionann an deasc dhrochúsáide in ISP agus post lánaimseartha amháin do FTE amháin nó (sa chuid is mó cásanna) do níos mó ná FTE amháin.

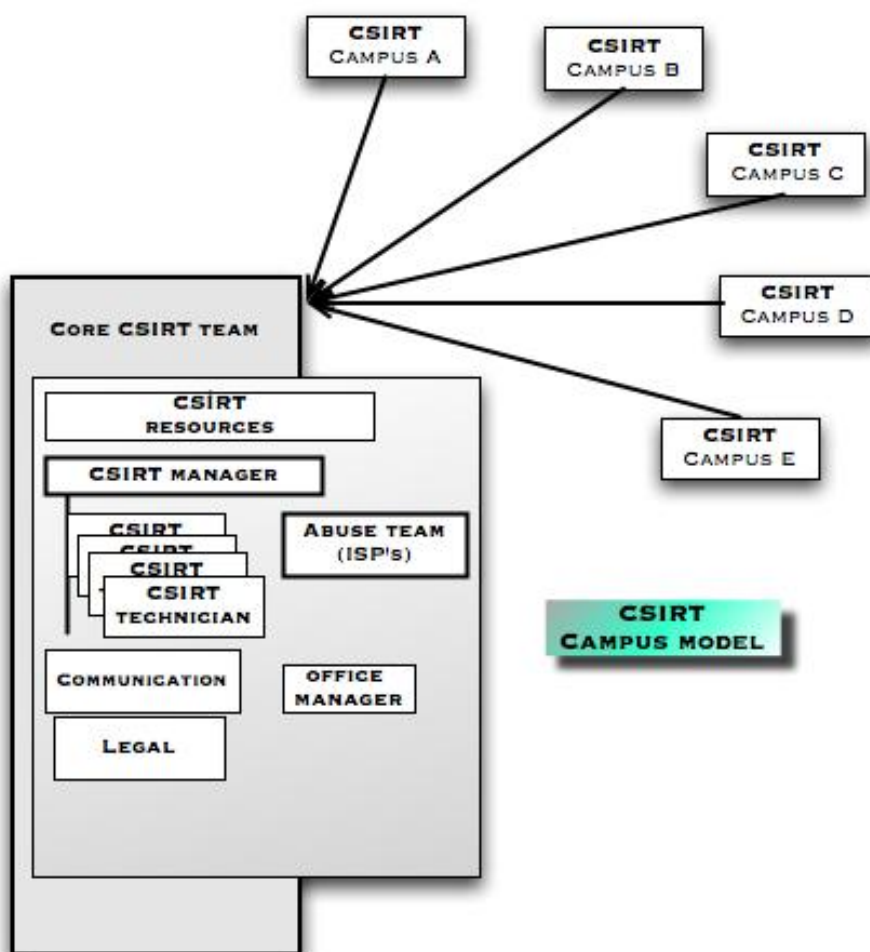


Fíor 6 Múnla leabaithe eagrúcháin

6.2.3 An múnla campais

De réir mar a chuirtear i bhfios leis an ainm, is é an múnla campais is minice a ghlactar le haghaidh CSIRT-anna acadúla agus taighde. Is é atá sa chuid is mó eagraíochtaí acadúla agus taighde ná ollscoileanna éagsúla agus saoráidí campais éagsúla in ionaid éagsúla agus iad scaipthe thar réigiún nó thar an tír ar fad (amhail na NREn-anna, is é sin le rá, na Gréasáin Náisiúnta Taighde). De ghnáth, bíonn na heagraíochtaí seo neamhspleách ar a chéile agus is minic a reáchtálann siad a CSIRT féin. De ghnáth, déantar na CSIRT-anna seo a eagrú faoi scáth an “máthair-CSIRT” nó an CSIRT lárnaigh. Déanann an CSIRT lárnach comhordú agus is é an pointe teagmhála aonair é don domhan mór. Sa chuid is mó cásanna, soláthróidh an CSIRT lárnach seirbhísí an CSIRT lárnaigh chomh maith le faisnéis maidir le teagmhais a scaipeadh chuig an CSIRT campais cuí.

Déanann roinnt CSIRT-anna a sheirbhísí lárnacha CSIRT a scaipeadh chuig na CSIRTanna campais eile, rud as a leanann forchostais níos ísle don CSIRT Lárnach.



Fíor 7 An múnla campais

6.2.4 An múnla saorálaigh

Is é atá sa mhúnla eagrúcháin seo ná grúpa daoine (speisialtóirí) a thagann le chéile chun comhairle agus tacaíocht a thabhairt dá chéile (agus do dhaoine eile) ar bhonn saorálach. Is comhphobal scaoilte é agus bíonn sé ag brath go mór ar dhíograis na rannpháirtithe.

Is é an múnla seo, mar shampla, a ghlac comhphobal WARP¹³.

6.3 An fhoireann cheart a earcú

Tar éis cinneadh a dhéanamh i dtaobh na seirbhísí agus an leibhéil tacaíochta atá le soláthar, agus tar éis múnla eagrúcháin a roghnú, is é atá sa chéad bheart eile ná an líon ceart daoine oile a aimsiú chun an obair a dhéanamh.

Tá sé beagnach dodhéanta figiúirí cruinne a sholáthar maidir leis an líon daoine teicniúla atá ag teastáil i dtaca leis seo de, ach tá cruthúnas ann gur cur chuige fónta na nithe seo a leanas:

- Chun dhá sheirbhís lárnacha a sholáthar maidir le feasacháin chomhairle a scaipeadh, mar aon le láimhseáil teagmhas: líon íosta **4** FTE.
- I gcomhair seirbhíse iomláine CSIRT le linn uaire oifige, agus chun córais a chothabháil: líon íosta **6 go 8** FTE.
- I gcás foime iomláine le haghaidh sheirbhís 24x7 (2 uain lasmuigh d'uaire oifige), is é atá sa líon íosta ná thart ar **12** FTE.

Áirítear sna huimhreacha sin iomarcaíochtaí freisin i gcomhair breoiteachta, laethanta saoire, etc. Tá sé riachtanach freisin seiceáil a dhéanamh maidir leis na comhaontaithe comhpháirteacha saothair atá ann. Dá mbeadh daoine ag obair lasmuigh d'uaire oifige, d'fhéadfadh sé go mbeadh sé sin ina chúis le costais bhreise i bhfoirm liúntas breise atá le híoc.

¹³ An tionscnamh WARP http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

Tar éis forléargas gairid a fháil ar na hinniúlachtaí tábhachtacha le haghaidh na saineolaithe teicniúla do CSIRT

Nithe ginearálta a bhaineann le cur síos ar phost mar dhuine d'fhoireann theicniúil:

Inniúlachtaí pearsanta

- Solúbtha, cruthaitheach agus meon maith foirne
- Scileanna maithe anailísithe
- Cumas chun ábhair dheacra theicniúla a mhíniú i bhfoclaíocht shimplí
- Tuiscint mhaith ar rúndacht agus ar obair a dhéanamh de réir nós imeachta áirithe
- Scileanna maithe eagrúcháin
- Ábaltacht maidir le déileáil le strus
- Scileanna maithe cumarsáide agus scríbhneoireachta
- Leathanaigeantach agus toilteanach nithe a fhoghlaim

Inniúlachtaí teicniúla

- Eolas leathan ar theicneolaíocht agus ar phrótacail idirlín
- Eolas ar chórais Linux agus Unix (de réir threalamh na cliantachta)
- Eolas ar chórais Windows (de réir threalamh na cliantachta)
- Eolas ar threalamh bonneagair gréasáin (Ródairí, lasca, DNS, Seachfhreastalaí, Ríomhphost, etc.)
- Eolas ar fheidhmiúcháin Idirlín (SMTP, HTTP(s), FTP, telnet, SSH, etc.)
- Eolas ar bhagairtí Slándála (DDoS, lascaireacht, Aghlot, smúrthacht, etc.)
- Eolas ar mheasúnú priacal agus ar chur i bhfeidhm praiticiúil

Inniúlachtaí breise

- Toilteanach a bheith ag obair ar sheal 24x7 nó ar glaoch (de réir an mhúnla seirbhíse)
- An oiread is mó is féidir i dtaca le hachar taistil (i gcás infhaighteachta éigeandála san oifig; am uasta taistil)
- An leibhéal oideachais
- Taithí ar obair i réimse na slándála IT

CSIRT samhailteach (beart 4)

An Plean Gnó a Phleanáil

An múnla airgeadais

Ó tharla go bhfuil ríomhgnó 24x7 ag an gcuideachta, mar aon le roinn IT 24x7, déantar cinneadh seirbhís iomlán a sholáthar le linn uaire oifige agus seirbhís ar ghlaoh a sholáthar lasmuigh d'uaire oifige. Déanfar na seirbhísí don chliantacht a sholáthar saor in aisce, ach déanfar an cumas maidir le seirbhísí a sholáthar do chustaiméirí seachtracha a mheasúnú le linn na céime píolóta agus na céime measúnachta.

An múnla ioncaim

Le linn na céime tosaigh agus na céime píolóta, déanfar an CSIRT a mhaoiniú tríd an gcuideachta óstach. Le linn na céime píolóta agus na céime measúnaithe déanfar maoiniú breise a phlé agus cuirfear san áireamh an seans go bhféadfaí seirbhísí a bheith á ndíol le custaiméirí seachtracha.

An múnla eagrúcháin

Is cuideachta bheag í an eagraíocht óstach agus, dá bhrí sin, roghnaítear an múnla leabaithe. Le linn uaire oifige, soláthróidh foireann triúr duine na seirbhísí lárnacha (ábhar comhairleach slándála a scaipeadh agus láimhseáil/comhordú teagmhas).

Tá daoine ag a bhfuil scileanna oiriúnacha ar fostú cheana féin ag roinn IT na heagraíochta. Déantar comhaontú leis an roinn sin ionas gur féidir an CSIRT nua tacaíocht a iarraidh ar bhonn ad-hoc nuair is gá sin. Chomh maith leis sin, is féidir leas a bhaint as an 2^ú líne dá dteicneoirí ar glaoch.

Beidh foireann lárnach CSIRT ann ina mbeidh ceathrar ball lánaimseartha agus cúigear ball breise CSIRT. Tá duine amháin díobh sin ar fáil freisin ar sheal athfhillteach.

Foireann

Tá cúlra ag ceannaire na foirne CSIRT i gcúrsaí slándála agus i dtacaíocht 1^ú agus 2^ú leibhéal agus tá taithí aige ar obair sa réimse bainistíochta athléimneachta i gcás géarchéimeanna. Is speisialtóirí slándála iad an triúr ball foirne eile. Tá baill foirne CSIRT páirtaimseartha na roinne IT ina speisialtóirí sa chuid de bhonneagar na cuideachta a bhaineann leo.

6.4 Úsáid agus trealamh na hoifige

Is ábhair an-leathan iad trealamh agus úsáid spáis oifige agus slándáil fhisiciúil agus, dá bhrí sin, ní féidir cur síos iomlán a sholáthar sa doiciméad seo. Tá an chaibidil ceaptha chun forléargas gairid a thabhairt faoin ábhar seo.

Is féidir tuilleadh faisnéise faoi shlándáil fhisiciúil a fháil ag na seoltaí seo a leanas:

http://en.wikipedia.org/wiki/Physical_security

http://www.sans.org/reading_room/whitepapers/physcial/

<http://www.infosyssec.net/infosyssec/physfac1.htm>

“An foirgneamh a láidriú”

Ó tharla go láimhseálann CSIRT-anna faisnéis an-íogair de ghnáth, is dea-chleachtas é ligean don fhoireann rialú a bheith acu ar shlándáil fhisiciúil na hoifige. Beidh sé sin ag brath ar na saoráidí láithreacha agus ar an mbonneagar láithreach agus ar pholasáí láithreach na cuideachta óstaí i ndáil le slándáil faisnéise.

Mar shampla, bíonn rialtais ag obair le scéimeanna aicmiúcháin agus bíonn siad an-dian i dtaca leis an tslí ina láimhseáiltear faisnéis rúnda. Déan seiceáil le do chuideachta nó le d’institiúid féin chun faisnéis a fháil faoi rialacha agus faoi pholasaithe áitiúla.

De ghnáth, bíonn ar CSIRT nua brath ar chomhoibriú óna eagraíocht óstach chun nithe a fhoghlaim faoi rialacha agus faoi pholasaithe áitiúla agus faoi shaincheistean dlíthiúla eile.

Ní thagann cur síos iomlán ar an trealamh agus ar na bearta slándála go léir a bheidh ag teastáil faoi réir raon an doiciméad seo. Tá liosta gairid anseo thíos, áfach, de na bunsaoaráidí le haghaidh do CSIRT:

Rialacha ginearálta don fhoirgneamh

- Rialuithe ar rochtain úsáide
- A chinntiú nach bhfuil an oifig CSIRT, ar a laghad, ar fáil ach amháin d'fhoireann CSIRT.
- Faireachán a dhéanamh ar oifigí agus ar bhealaí isteach trí cheamairí a úsáid.
- Faisnéis rúnda a chartlannú i locair nó i dtaisceadán.
- Córais dhaingne IT a úsáid.

Rialacha ginearálta maidir le trealamh IT

- Trealamh a úsáid a bhfuil tacaíocht na foirne ann ina leith
- Gach córas a láidriú
- Do chuid córas go léir a phaisteáil agus a uasdátú sula gcuirtear i gceangal leis an idirlíon iad
- Bogearraí slándála a úsáid (ballaí dóiteáin, scanóirí iolracha frithviris, earraí frithspiaireachta, etc.)

Bealaí cumarsáide a chothabháil

- Láithreán Gréasáin Poiblí
- Limistéar dúnta ar an Láithreán Gréasáin i gcomhair ball
- Foirmeacha gréasáin chun teagmhais a thuairisciú
- Ríomhphost (tacaíocht PGP / GPG / S/MIME)
- Bogearraí liosta seoltaí ríomhphoist
- Sainuimhir theileafóin a bheith ar fáil don chliantacht:
 - Fón
 - Facs
 - SMS

Córa(i)s rianaithe taifead

- Bunachar sonraí teagmhála ina bhfuil mionsonraí faoi bhaill foirne, faoi fhoirne eile, etc.
- Uirlisí CRM
- Córas ticéad láimseála teagmhas

An “stíl chorparáideach” a úsáid ón tús maidir leis na nithe seo a leanas

- Leagan amach caighdeánach le haghaidh ríomhphoist agus feasacháin chomhairligh
- Litreacha páipéir ‘seanfhaiseanta’
- Tuarascálacha míosúla nó tuarascálacha bliantúla
- Foirm thuairiscithe teagmhas

Saincheisteanna eile

- Cumarsáid as-banda a thuar i gcás ionsaithe
- Iomarcaíocht a thuar maidir le nascacht idirlín

Chun tuilleadh faisnéise a fháil faoi uirlisiú sonrach CSIRT, féach caibidil 8.5 *Uirlisiú CSIRT atá ar fáil*.

6.5 Polasaí slándála faisnéise a fhorbairt

Ag brath ar an gcineál CSIRT atá ann, beidh sainpholasaí slándála faisnéise agat. Ar leith ó chur síos a dhéanamh ar staid inmhiannaithe na bpróiseas agus na n-ósanna imeachta oibríochta agus riaracháin, ní mór go mbeadh an polasaí sin i gcomhréir le reachtaíocht agus le caighdeáin, go háirithe maidir le dlíteanas an CSIRT. De ghnáth, bíonn an CSIRT faoi cheangal ag dlíthe agus ag rialacháin náisiúnta a chuirtear i bhfeidhm go minic i gcomhthéacs reachtaíochta Eorpaí (Treoracha de ghnáth) agus comhaontuithe idirnáisiúnta eile. Ní gá go mbeadh caighdeáin ceangailteach go díreach ach is féidir iad a shainordú nó a mholadh le dlíthe nó le rialacháin.

Anseo thíos, gheofar liosta gearr de dhlíthe agus de pholasaithe ionchasacha:

Náisiúnta

- Dlíthe éagsúla ar theicneolaíocht eolais, ar theileachumarsáid, ar na meáin
- Dlíthe maidir le cosaint sonraí agus príobháideacht
- Dlíthe agus rialacháin maidir le coimeád sonraí
- Reachtaíocht maidir le hairgeadas, cuntasáíocht agus bainistíocht chorporáideach
- Cóid iompair i gcomhair rialachais chorporáidigh agus rialachais IT

Eorpach

- Treoir ar shínithe leictreonacha (1999/93/EC)
- Treoracha ar chosaint sonraí (1995/46/EC) agus ar phríobháideacht i gcumarsáid leictreonach (2002/58/EC)
- Treoracha ar ghréasáin agus ar sheirbhísí cumarsáide leictreonaí (2002/19/EC – 2002/22/EC)
- Treoracha ar Dhlí Cuideachta (e.g. 8^ú Treoir Dlí Cuideachta)

Idirnáisiúnta

- Comhaontú Basel II (go háirithe maidir le bainistiú priacal oibríochta)
- Coinbhinsiún Chomhairle na hEorpa ar Chibearchoireacht
- Coinbhinsiún Chomhairle na hEorpa ar Chearta an Duine (airteagal 8 maidir le phríobháideacht)
- Caighdeáin Idirnáisiúnta maidir le Cuntasáíocht (IAS; déantar rialuithe IT a shainordú leo go feadh méid áirithe)

Caighdeáin

- Caighdeán Briotanach BS 7799 (Slándáil Faisnéise)
- Caighdeáin Idirnáisiúnta ISO2700x (Córais Bhainistíochta Slándála Faisnéise)
- IT-Grundschutzbuch na Gearmáine, EBIOS na Fraince agus malairtí náisiúnta eile

Chun cinneadh a dhéanamh i dtaobh an bhfuil CSIRT s'agatsa ag gníomhú de réir reachtaíochta náisiúnta agus idirnáisiúnta, téigh i dteagmháil le do chomhairleoir dlí le do thoil.

Seo a leanas na ceisteanna is bunúsaí atá le freagairt i dtaca le do pholasaithe láimhseála faisnéise:

- Conas a dhéantar faisnéis isteach “a lipéadú” nó “a aicmiú”?
- Conas a láimhseáiltear faisnéis, go háirithe i dtaca le heisiachas?
- Cad iad na nithe a bhreithnítear i dtaca le nochtadh faisnéise, go háirithe an ndéantar faisnéis a bhaineann le teagmhais a chur ar aghaidh chuig foirne nó láithreáin eile?
- An bhfuil aon ábhar dlíthiúil le cur i gcuntas maidir le láimhseáil faisnéise?
- An bhfuil polasaí agat maidir le húsáid cripteolaíochta chun eisiachas & iomláine a chosaint in ábhair chartlainne agus/nó i gcumarsáid sonraí, go háirithe ríomhphost?
- An bhfuil san áireamh sa pholasaí seo coinníollacha ionchasacha teorann dlí ar nós ábhair a thaisceadh le tríú páirtí nó infhorfheidhmitheacht an díchríptithe i gcás agraí dlí a bheith ann.

CSIRT samhailteach (beart 5)

Trealamh agus suíomh na hoifige

Ó tharla go bhfuil slándáil fhisiciúil éifeachtúil i bhfeidhm ag an gcuideachta óstach, tá an CSIRT nua clúdaithe go maith i dtaca leis sin de. Soláthraítear seomra ar a dtugtar “seomra cogaidh” le gur féidir comhordú a dhéanamh i gcás éigeandála. Ceannaítear taisceadán le haghaidh an ábhair criptiúcháin agus le haghaidh doiciméad fogair. Bunaíodh líne theileafóin ar leithligh, lena n-áirítear lasc-chlár mar éascaíocht i gcomhair líne éigeandála le linn uaire oifige, agus fón póca dualgais shoghluaiste “ar glaoch” le haghaidh amanna lasmuigh d’uaire oifige, agus an uimhir chéanna aige leis an líne éigeandála.

Is féidir trealamh láithreach agus an láithreán gréasáin corparáideach le haghaidh fógartí a bhaineann le CSIRT a úsáid freisin. Déantar liosta seoltaí poist a shuiteáil agus a chothabháil agus tá cuid shrianta ann le haghaidh cumarsáidí idir ceannairí foirne agus le foirne eile. Déantar na mionsonraí go léir faoi bhaill foirne a stóráil i mbunachar sonraí agus coimeádtar leagan clóite sa taisceadán.

Rialáil

Ó tharla go bhfuil an CSIRT leabaithe i gcuideachta ag a bhfuil polasaithe slándála cheana féin, bunaíodh na polasaithe rochtana don CSIRT a bhunú le cabhair ó chomhairleoir dlí na cuideachta.

6.6 Comhoibriú a lorg idir CSIRT-anna eile agus tionscnaimh ionchasacha náisiúnta

Rinneadh tagairt cúpla uair cheana féin sa doiciméad seo do thionscnaimh eile CSIRT eile a bheith ann agus don ghá mór le comhoibriú eatarthu. Is dea-chleachtas é teagmháil a dhéanamh a luaite is féidir le CSIRT-anna eile chun an caidreamh riachtanach a bhunú le comhphobail CSIRT. De ghnáth, bíonn CSIRT-anna an-oscailte i dtaca le cabhair a thabhairt d’fhoirne nua-cheaptha dul i mbun oibre.

Is pointe tosaigh an-mhaith é *Inventory of CERT activities in Europe*¹⁴ le ENISA i ndáil

¹⁴ Fardal ENISA: http://www.enisa.europa.eu/cert_inventory/

leis an gcuardach ar CSIRT-anna eile sa tír nó le haghaidh gníomhaíochtaí comhoibrithe de chuid CSIRT-anna náisiúnta.

Chun tacaíocht a fháil maidir le foinse oiriúnach faisnéise faoi CSIRT, déan teagmháil le saineolaithe ENISA ar chúrsaí CSIRT:

cert-relations@enisa.europa.eu

Tar éis forléargas ar ghníomhaíochtaí comhphobail CSIRT. Féach an *Inventory* le do thoil chun cur síos níos cuimsithí agus tuilleadh faisnéise a fháil.

Tionscnamh CSIRT Eorpach

TF-CSIRT¹⁵

Déanann an Tasc-Fhórsa TF-CSIRT comhoibriú idir Foirne Freagartha Teagmhas Slándála Ríomhaire (CSIRT-anna) san Eoraip a chur chun cinn. Is é atá i bpríomhaidhmeanna an Tasc-Fhórsa sin ná fóram a sholáthar chun taithí agus eolas a mhalartú, chun seirbhísí píolóta a bhunú do chomhphobal na CSIRT-anna Eorpacha agus chun cúnamh a thabhairt maidir le bunú CSIRT-anna nua.

Is iad seo a leanas príomhaidhmeanna an Tasc-Fhórsa:

- Fóram a sholáthar chun taithí agus eolas a mhalartú
- Seirbhísí píolóta a bhunú don phobal CSIRT-anna Eorpacha
- Caighdeán agus nósanna imeachta coiteanna a chur chun cinn chun gníomhú nuair a tharlaíonn teagmhais slándála
- Cúnamh a thabhairt maidir le bunú CSIRT-anna nua agus foireann CSIRT-anna a oiliúint.
- Tá gníomhaíochtaí TF-CSIRT dírithe ar an Eoraip agus ar thíortha comharsanacha, i gcomhlíonadh na dTearmaí Tagartha arna gceadú ag Coiste Teicniúil TERENA Technical Committee ar an 15 Meán Fómhair 2004.

Tionscnamh CSIRT domhanda

FIRST¹⁶

Is é atá in FIRST ná an phríomheagraíocht agus an ceannaire aitheanta domhanda i dtaca le freagairt teagmhas. Trí bhallraíocht in FIRST, tá foirne freagartha in ann freagairt níos éifeachtaí a dhéanamh i gcás teagmhas slándála – ar shlí fhreagarthach agus ar shlí ghníomhaíoch araon.

Déanann FIRST foirne éagsúla freagartha teagmhas ríomhaire a thabhairt le chéile ó eagraíochtaí rialtais, tráchtála agus oideachais. Is é aidhm FIRST comhoibriú agus comhordú a chothú i ndáil le cosc teagmhas, freagairt mhear a spreagadh i gcás teagmhas, agus comhroinnt faisnéise i measc ball agus an chomhphobail i gcoitinne a spreagadh.

Ar leith ón ngréasán iontaoibhe a bhíonn ann sa chomhphobal domhanda freagartha

¹⁵ TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

¹⁶ FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm



teagmhas de thoradh FIRST, soláthraíonn FIRST seirbhísí breisluacha freisin.

CSIRT samhailteach (beart 6)

Comhoibriú a lorg

Trí Fhardal ENISA a úsáid go tapa, rinneadh roinnt CSIRT-anna sa tír chéanna a aimsiú agus rinneadh teagmháil leo. Socraíodh cuairt láithreáin le ceann amháin acu don cheannaire foirne a bhíodhas tar éis a earcú. D'fhoghlaim sé faoi ghníomhaíochtaí náisiúnta CSIRT agus d'fhreastail sé ar chruinniú.

Bhí an cruinniú sin thar a bheith cuiditheach maidir le samplaí a bhailiú de mhodhanna oibre agus maidir le tacaíocht a fháil ó chúpla foireann eile.

7. An Plean Gnó a Chur Chun Cinn

Tá na bearta seo a leanas déanta againn go dtí seo:

1. Tuiscint a fháil ar céard é CSIRT agus cé na tairbhí a d'fhéadfadh a bheith ann dá bharr.
2. Cén earnáil a soláthróidh an fhoireann nua a cuid seirbhísí di?
3. Cad iad na cineálacha seirbhísí atá CSIRT in ann a sholáthar dá chliantacht.
4. Anailís a dhéanamh ar an timpeallacht agus ar na cliaint
5. An ráiteas misin a shainmhíniú
6. An Plean Gnó a Fhorbairt
 - a. An múnla airgeadais a shainmhíniú
 - b. An múnla eagrúcháin a shainmhíniú
 - c. Tús a chur le hearcú foirne
 - d. Úsáid agus trealmhú na hoifige
 - e. Polasaí slándála faisnéise a fhorbairt
 - f. Comhpháirtithe comhoibrithe a chuardach

>> Is é atá sa chéad bheart eile ná an méid sin thuas a chur isteach i bplean tionscadail agus tús a chur leis an obair!

Tús maith maidir le do thionscadal a shainmhíniú is ea cás gnó a cheapadh. Úsáidfear an cás gnó sin mar bhonn le haghaidh an phlean tionscadail agus úsáidfear é freisin le linn iarratas a dhéanamh ar thacaíocht ón lucht bainistíochta agus ar buiséad nó acmhainní eile.

Tá cruthúnas ann a léiríonn go raibh sé úsáideach tuairiscí a thabhairt ar bhonn buan don lucht bainistíochta d'fhonn ardleibhéal feasachta a choimeád ar bun i dtaca le fadhbanna slándála IT agus, ar an dóigh sin, d'fhonn tacaíocht leanúnach a fháil le haghaidh an CSIRT áitiúil.

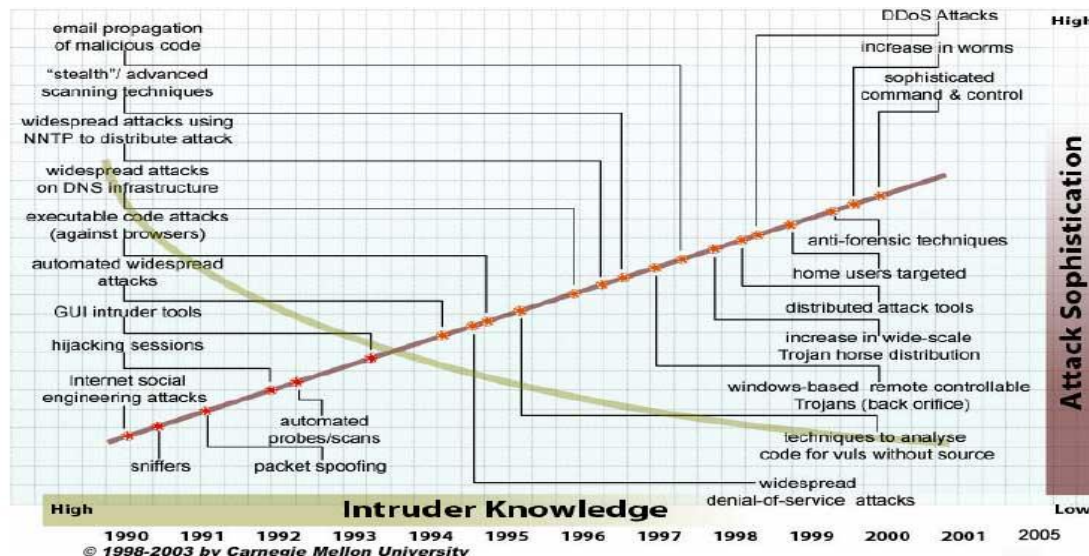
Chun tús a chur le cás gnó, is ceart anailís a dhéanamh ar na fadhbanna agus ar na deiseanna trí leas a bhaint as an múnla anailíse a thuairiscítear i gcaibidil 5.3 *Anailís ar an gCliantacht*, agus dlúth-theagmháil a chuardach leis an gcliantacht ionchasach.

De réir mar a thuairiscítear roimhe seo, tá a lán ábhair machnaimh ann nuair atá tús a chur le CSIRT. Is fearr an t-ábhar thuasluaite a oiriúnú do riachtanais an CSIRT de réir mar a thagann siad chun cinn.

Is dea-chleachtas é, le linn tuairisciú don lucht bainistíochta, an cás gnó a bheith chomh cothrom le dáta agus is féidir trí leas a bhaint as ailt a bhí sna nuachtáin nó ar an idirlíon le déanaí agus trí mhíniú a thabhairt i dtaobh cén fáth go bhfuil seirbhís CSIRT agus comhordú inmheánach teagmhas chomh tábhachtach sin maidir le sócmhainní i gcomhair gnó dhaingin. Tá sé riachtanach freisin go mbeadh sé soiléir gur trí thacaíocht leanúnach do nithe a bhaineann le slándáil IT, agus tríd an tacaíocht sin amháin, a bhaintear gnó cobhsaí amach, go háirithe i gcás cuideachta nó institiúide atá spleách ar IT.

(Léiríonn abairt choitianta de chuid Bruce Schneier an méid sin, is é sin le rá: “Security is not a product but a process¹⁷!”)

Uirlis iomráiteach maidir le léiriú a thabhairt ar fhadhbanna slándála is ea an graf seo a leanas arna sholáthar ag CERT/CC:



Fíor 8 Eolas faoi ionróirí i gcomparáid le sofaisticiúlacht ionsaithe (foinse CERT-CC¹⁸)

Samhlaítear leis an uirlis seo na treochtaí i dtaca le slándáil IT, go háirithe an laghdú ar na scileanna riachtanacha chun ionsaithe a dhéanamh atá ag éirí níos sofaisticiúla i gcónaí.

Pointe eile is fiú a lua ná an tréimhse laghdaitheach ama atá ann idir bogearraí uasdátaithe a bheith ar fáil i gcomhair leochaileachaí agus tús a chur le hionsaithe ina n-aghaidh:

Paiste -> Teagmhas

Nimda: 11 mhí
Slammer: 6 mhí
Nachi: 5 mhí
Blaster: 3 seachtaine
Witty: 1 lá (!)

Ráta leata

Code red: Laethanta
Nimda: Uaireanta an chloig
Slammer: Nóiméid

Léiriú maith freisin is ea sonraí atá bailithe faoi theagmhas, feabhsúcháin ionchasacha agus na ceachtanna a foghlaimíodh.

¹⁷ Bruce Schneier: <http://www.schneier.com/>

¹⁸ <http://www.cert.org/archive/pdf/info-sec-ip.pdf>

7.1 *Cur síos ar phleananna gnó agus ar thruicir bhainistíochta*

Ní leo cur i láthair don lucht bainistíochta, lena n-áirítear CSIRT a chur chun cinn, chun cás gnó a dhéanamh ach má dhéantar an méid sin ar mhodh cuí leanfaidh tacaíocht ón lucht bainistíochta as sa chuid is mó cásanna. Ní ceart a mheas gurb é atá sa chás gnó ná rud atá le déanamh don lucht bainistíochta ach is ceart é a úsáid freisin chun faisnéis a chur in iúl don fhoireann agus don chliantacht. Tá cuma an-tráchtálach ar an téarma 'cás gnó', b'fhéidir, agus is téarma é nach bhfuil baint mhór aige le gnó laethúil CSIRT, ach soláthraíonn sé fócas maith agus treoir mhaith le linn CSIRT a chur ar bun.

D'fhéadfaí na freagraí ar na ceistanna seo a leanas a úsáid chun cás gnó maith a dhearadh (tá na samplaí a thugtar hipitéiseach agus is mar léiriú amháin a thugtar iad. Bíonn na "fíor-fhreagraí" ag brath go mór ar na "fíor-imthosca").

- Céard é an fhadhb?
- Cad ba mhaith leat a bhaint amach in éineacht le do chliant?
- Cad a tharlaíonn mura ndéanann tú aon bheart?
- Cad a tharlaíonn má dhéanann tú beart?
- Cén costas a bheidh ann?
- Cad a ghnóthófar?
- Cathain a thosaíonn tú agus cén uair atá sé críochnaithe?

Céard é an fhadhb?

Sa chuid is mó cásanna, tagann an smaoineamh maidir le CSIRT a chur ar bun chun cinn nuair atá slándáil IT tar éis teacht chun bheith ina chuid riachtanach de ghnó lárnach cuideachta nó institiúide agus nuair a thagann teagmhais slándála chun bheith ina bpríacal gnó, rud a fhágann gur gnáthoibríocht ghnó é maolú deacrachtaí slándála.

I gcás an chuid is mó cuideachtaí nó institiúidí, bíonn roinn tacaíochta rialta nó deasc chabhrach acu ach sa chuid is mó cásanna láimhseáiltear le teagmhais slándála ar mhodh neamhdhóthanach agus ní ar mhodh struchtúrtha de réir mar is ceart. Sa chuid is mó cásanna, bíonn scileanna agus aird speisialta ag teastáil sa réimse oibre a bhaineann le teagmhais slándála. Tá tairbhe ag gabháil le cur chuige níos struchtúrtha freisin agus maolófar priacail ghnó agus damáiste don chuideachta.

Sa chuid is mó cásanna, is é atá san fhadhb ná go bhfuil easpa comhordaithe ann agus nach n-úsáidtear an t-eolas láithreach chun teagmhais a láimhseáil, rud a d'fhéadfadh cosc a chur ar na teagmhais tarlú sa todhchaí agus cosc a chur ar na caillteanais ionchasacha airgeadais agus/nó ar dhamáiste do chlú institiúide.

Cad iad na haidhmeanna atá le baint amach in éineacht leis an gcliantacht?

Mar a míníodh níos túisce, fónfaidh do CSIRT dá chliant agus cabhróidh sé leo i dtaca le teagmhais agus fadhbanna slándála a réiteach. Is aidhmeanna breise iad méadú a dhéanamh ar leibhéal an eolais faoi shlándáil IT agus cultúr feasachta slándála a chruthú.

De bharr cultúir den sórt sin, déantar bearta gníomhaíocha agus bearta coisctheacha ón tús agus, dá bhrí sin, laghdaítear costais oibríochta.

Má thugtar cultúr an chomhoibrithe agus an chúnaimh isteach i gcuideachta nó in institiúid, is é a tharlaíonn, sa chuid is mó cásanna, ná éifeachtúlacht a spreagadh i gcoitinne.

Cad a tharlaíonn mura ndéantar aon bheart?

D'fhéadfadh sé tarlú, i gcás bealach neamhstruchtúrtha a bheith ann chun slándáil IT a láimhseáil, go mbeidh tuilleadh damáiste ann, go háirithe do chlú na hinstitiúide. D'fhéadfadh caillteanais airgeadais agus impleachtaí dlíthiúla a bheith ann freisin.

Cad a tharlaíonn má dhéantar beart?

Méadaítear an fheasacht maidir le líon na bhfadhbanna slándála a bhíonn ann. Is cabhair é sin i dtaca leis na fadhbanna sin a réiteach ar bhealach níos éifeachtúla agus i dtaca le tuilleadh caillteanais a chosc sa todhchaí.

Cén costas a bheidh ann?

Ag brath ar chineál na heagraíochta, cosnóidh sé tuarastail bhaill foirne an CSIRT mar aon le costais eagrúcháin, trealaimh, uirlisithe agus ceadúnas bogearraí.

Cad a ghnóthófar?

Ag brath ar an ngnó agus ar na caillteanais a tharla san am atá caite, gnóthófar tuilleadh trédhearcachta maidir le nósanna imeachta agus cleachtais slándála, agus, dá bhrí sin, beidh sócmhainní riachtanacha gnó á gcosaint.

Céard é an t-amlíne?

Féach caibidil 12. *Cur síos ar an bplean Tionscadail* chun cur síos a fháil ar phlean samplach tionscadail.

Samplaí de chásanna agus cur chuige gnó atá ann cheana féin

Seo a leanas roinnt samplaí de chásanna gnó CSIRT agus is fiú staidéar a dhéanamh orthu:

- http://www.cert.org/csirts/AFI_case-study.html

CSIRT de chuid Institiúide Airgeadais a Chruthú: Cás-Staidéar

Is é is cuspóir don doiciméad seo ná ceachtanna a chomhroinnt a d'fhoghlaim institiúid airgeadais (dá ngairtear AFI sa doiciméad seo) de réir mar a bhí siad ag forbairt agus ag cur i bhfeidhm plean chun aghaidh a thabhairt ar ábhair imní slándála agus Foirne Freagartha Teagmhas Slándála Ríomhaire (CSIRT).

- <http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf>

Achoimre ar chás gnó CERT POLSKA (léiriú sleamhnán i bhformáid PDF).

- <http://www.auscert.org.au/render.html?it=2252>

Le linn bhlianta na 1990-idí, d'fhéadfadh deacrachtaí a bheith ann i dtaca le Foireann Freagartha Teagmhas (IRT) a fhoirmiú. Ní bhíonn aon taithí ar an gcineál seo taisc ag a lán daoine a fhoirmíonn IRT. Sa pháipéar seo, déantar scrúdú ar an ról a d'fhéadfadh a bheith ag IRT sa chomhphobal agus ar na saincheistanna ar ceart aghaidh a thabhairt orthu nuair atá an foirmiú ar siúl agus tar éis tús a chur le

hoibríochtaí. D'fhéadfadh sé a bheith ina chabhair freisin do IRT-anna atá ann cheana féin mar d'fhéadfadh sé go soláthróidh sé eolas faoi shaincheistean nár tugadh aghaidh orthu roimhe seo.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
Cás-Staidéar maidir le Slándáil Faisneise, An Fiontar a Dhaingniú, le: Roger Benton

Seo cás-staidéar praiticiúil ar an aistriú a rinne Cuideachta Árachais chuig córas slandála uile-fhiontair. Is é atá beartaithe leis an staidéar praiticiúil seo na conair a sholáthar ata le leanúint le linn córas slandála a chruthú nó le linn aistriú chuig córas slandála. I dtosach, ba é an t-aon mheicníocht a bhí ann chun rochtain a fháil ar shonraí corparaideacha ná córas bunata slandála ar-líne. Bhí na contúirtí an-mhór – ní raibh aon rialuithe iomláine ann lasmuigh den timpeallacht ar-líne. Bheadh aon duine ag a raibh bunscileanna ríomhchlárúchain aige nó aici in ann sonraí tairgeachta a chur isteach, a athrú agus/nó a scriosadh.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
Straitéis ríomhshlandála Marriott: comhoibriú ghnó IT

Próiseas, seachas tionscadal, atá i dtaithí Chris Zoladz, as Marriott International, Inc., ar ríomhshlandáil. Ba é sin an teachtaireacht a thug Zoladz ag Comhdháil agus Taispeántas Ríomhshlandála a bhí ann le déanaí faoi choimirce an Intermedia Group. Ina chail mar leas-uachtarán na cosanta faisnéise in Marriott, déanann Zoladz tuairisciú tríd an roinn dlí, d'ainneoin nach dlíodóir é. Is é atá san fheidhm atá aige ná a shainaithint cén ait ina stóraithear an fhaisnéis ghnó is luachmhaire de chuid Marriot agus conas a ghluaiseann sí laistigh den chuideachta agus lasmuigh di. Tá freagracht ar leithligh ag Marriott ar freagracht í arna sainmhíniú le haghaidh an bhonneagair theicniúil atá ann mar thacaíocht do shlandáil agus leagtar an fhreagracht sin ar an ailtire slandála IT.

CSIRT samhailteach (beart 7)

An Plean Gnó a Chur Chun Cinn

Déantar cinneadh chun fórais agus figiúirí a bhailiú ó stair na cuideachta. Tá se sin thar a bheith úsáideach i dtaca le forléagas staitisticiúil ar an staid slandála IT. Is ceart leanúint den bhailiú sin nuair atá an CSIRT faoi lánseo d'fhonn na staitisticí a choimeád cothrom le dáta.

Rinneadh teagmháil le CSIRT-anna náisiúnta eile agus rinneadh agallaimh leo faoina gcuid cásanna gnó. Rinne siad tacaíocht a sholáthar trí roinnt sleamhnan a thiomsú ina raibh faisnéis faoi forbairtí le déanaí maidir le teagmhais slandála IT agus faoi chostais teagmhas.

Sa chás samplach seo de CSIRT Samhailteach, ní raibh aon ghá mór lena áiteamh ar an lucht bainistíochta cé chomh tábhachtach ata gnó IT, agus, dá bhrí sin, ní raibh sé deacair ceadú a fháil don chéad chéim. Rinneadh cás gnó agus plean tionscadail a ullmhú, lena n-áirítear meastachán ar na costais tosaithe agus costas na hoibríochta.

8. Samplaí de nósanna imeachta oibríochta agus teicniúla (sreabhadh oibre)

Tá na bearta seo a leanas déanta againn go dtí seo:

1. Tuiscint a fháil ar céard é CSIRT agus cé na tairbhí a d'fhéadfadh a bheith ann dá bharr.
2. Cén earnáil a soláthróidh an fhoireann nua a cuid seirbhísí di?
3. Cad iad na cineálacha seirbhísí atá CSIRT in ann a sholáthar dá chliantacht.
4. Anailís a dhéanamh ar an timpeallacht agus ar na cliaint
5. An ráiteas misin a shainmhíniú
6. An Plean Gnó a Fhorbairt
 - a. An múnla airgeadais a shainmhíniú
 - b. An múnla eagrúcháin a shainmhíniú
 - c. Tús a chur le hearcú foirne
 - d. Úsáid agus trealmhú na hoifige
 - e. Polasaí slándála faisnéise a fhorbairt
 - f. Comhpháirtithe comhoibrithe a chuardach
7. An Plean Gnó a Chur Chun Cinn.
 - a. Ceadú a fháil don chás gnó.
 - b. Gach rud a chur isteach i bplean tionscadail.

>> Is é atá sa chéad bheart eile ná: an CSIRT a chur i bhfeidhm

Má bhíonn sreabhadh oibre dea-shainmhínithe ann, is amhlaidh a chuirfear feabhas ar chaighdeán is amhlaidh is fearr a bheidh an t-am atá ag teastáil i gcomhair gach teagmhais nó cáis leochaileachta.

Mar a thuairiscítear sna boscaí sna samplaí, tairgeoidh CSIRT Samhailteach na bunseirbhísí lánacha CSIRT:

- Folairimh agus Rabnhaidh
- Laimhseáil Teagmhas
- Fógairtí

Sa chaibidil seo, tugtar samplaí de shreabhadh oibre ina dtuairiscítear seirbhísí lánacha CSIRT. Sa chaibidil seo freisin, tá faisnéis le fáil maidir le bailiú faisnéise ó fhoinsí eagsúla, á seiceáil de réir ábharthachta agus fíre agus á athdháileadh ar an gcliantacht. Agus sa deireadh, tá samplaí le fáil sa chaibidil seo de na nósanna imeachta is bunúsaí agus d'uirlisiú sonracha CSIRT.

8.1 *Bonn suiteála na cliantachta a mheasúnú*

Is é atá sa chéad chéim ná forléargas a bhailiú faoi na córais IT ata suiteailte i do chliantacht. Ar an dóigh sin, is féidir leis an CSIRT measúnú a dhéanamh ar ábharthacht faisneise isteach agus an fhaisnéis sin a scagadh roimh athdháileadh agus, dá bhrí sin, ní bhfaighidh na cliant rabharta mhór faisnéise nach mbaineann leo ar aon slí.

Is dea-chleachtas é tosú ar bhealach simplí, mar shampla trí úsaid a bhaint as leathán excel den sórt seo a leanas:

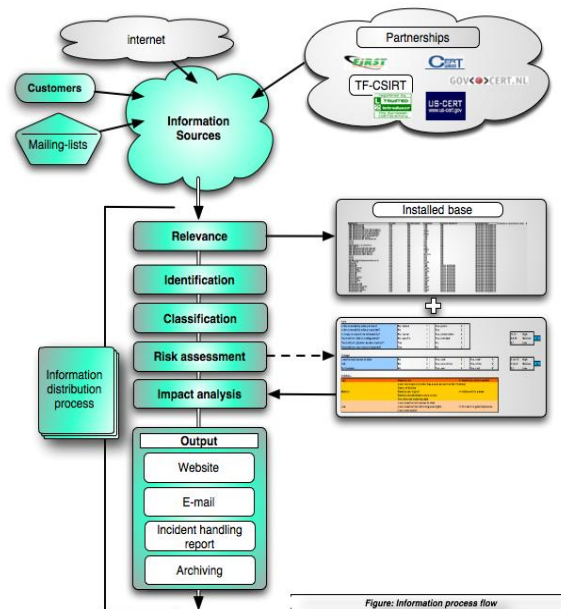
Catagóir	Feidhmiúchán	Tairge bogearraí	Leagan	OS version	OS	Cliant
Deasc	Office	Excel	x-x-x	Microsoft	XP-prof	A
Deasc	Brabhsalaí	IE	x-x-	Microsoft	XP-prof	A
Gréasán	Ródaire	CISCO	x-x-x	CISCO	x-x-x-	B
Freastalaí	Freastalaí	Linux	x-x-x	L-distro	x-x-x	B
Seirbhísí	Freastalaí gréasain	Apache		Unix	x-x-x	B

Trí leas a bhaint as feidhm scagtha excel, tá sé an-éasca na bogearraí cearta a roghnú agus a fháil amach cé na cliant éagsúla a úsáideann bogearraí éagsúla áirithe.

8.2 Foláirimh, Rabhaidh agus Fógairtí a Ghiniúint

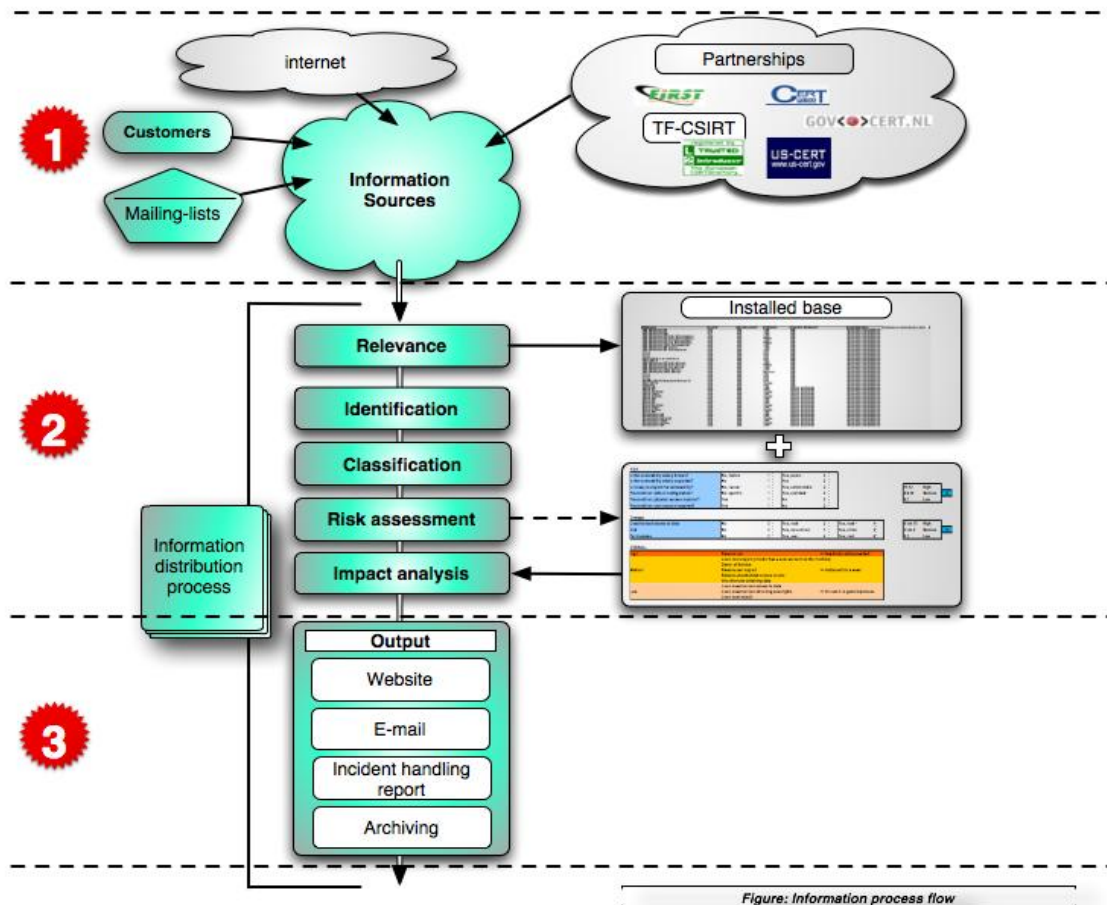
Is de réir an tsreafa oibre chéanna a ghintear foláirimh, rabhaidh agus fógairtí:

- Faisnéis a bhailiú
- An fhaisnéis a mheasúnú maidir le hábharthacht agus foinse
- Measúnú priacal atá bunaithe ar an bhfaisnéis a bailíodh
- An fhaisnéis a dháileadh



Fíor 9: Sreabhadh próisis faisnéise

Déanfar an sreabhadh oibre seo a thuairisciú ar shlí níos mionsonraithe sna míreanna sin ina dhiaidh seo.



1

Beart 1: Faisnéis leochaileachta a bhailiú.

De ghnáth, bíonn dhá phríonhchineal foinse faisnéise ann atá ina gcabhair maidir le faisnéis a úsáid mar ionchur do na seirbhísí:

- Faisneis leochaileachta maidir le córais IT (s'agatsa)
- Tuairiscí faoi theagmhais

Ag brath ar an gcineál gnó agus ar an gcineál bonneagair IT, tá a lán foinsí poiblí agus foinsí dúnta ann i gcomhair faisnéise leochaileachta:

- Liostaí seoltaí poist, idir phoiblí agus dhúnta
- Leochaileacht díoltóirí agus faisnéis faoi tháirgí
- Laithreáin ghréasáin
- Faisneis ar an Idirlíon (Google, etc...)
- Comhphairtíochtaí poiblí agus príobháideacha a sholáthraíonn faisnéis faoi leochaileacht (FIRST, TF-CSIRT, CERT-CC, US-CERT....)

Ta an fhaisnéis sin go léir ina cabhair maidir leis an leibhéal eolais faoi leochaileachtaí sonracha i gcórais IT.

Mar atá luaite roimhe seo, tá a lán foinsí maithe sorochtana faisnéise ar fáil ar an idirlíon. Tráth scríofa an doiciméid seo, tá liosta níos cuimsithí á sholáthar ag grúpa oibre ad-hoc ENISA, “seirbhísí CERT” do 2006, ar liosta é atá in ainm a bheith réidh faoi dheireadh na bliana 2006¹⁹.

Beart 2: An fhaisnéis a mheasúnú agus an priacal a mheas

Is é a leanfaidh as an mbeart seo ná anailís ar an tionchar atá ag leochaileacht shonrach ar bhonneagar IT na cliantachta.

Sainaithint

Ní mór faisnéis leochaileachta isteach a shainaithint i gcónaí trína foinse agus ní mór a chinneadh i gcónaí an bhfuil an fhoinsé iontaofa sula dtugtar aon fhaisnéis don chliantacht. Thairis sin, d’fhéadfadh sé go dtabharfaí foláirimh bhréige do dhaoine, rud as a leanfadh suaithheadh gan ghá i bpróisis ghnó agus, sa deireadh, damáiste do chlú an CSIRT.

¹⁹ Seirbhísí ad-hoc WG CERT: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Sa nós imeachta seo a leanas, taispeántar sampla a bhaineann le fíre teachtaireachta a shainaithint:

Nós imeachta ar tríd a shainaithneofar fíre teachtaireachta agus a foinse Seicliosta Ginearalta

1. An bhfuil an foinse ar eolas agat agus an bhfuil sí cláraithe mar foinse den sórt sin?
2. An dtagann an fhaisnéis trí bhealach rialta?
3. An bhfuil faisnéis “aisteach” ann a bhfuil cuma “mícheart” uirthi?
4. Déan de reir do mhothúcháin, má tá ábhar amhrais ann faoi fhaisnéis áirithe ná gníomhaigh ina leith ach fíoraigh arís í!

Ríomhphost - Foinsí

1. An bhfuil seoladh na foinse ar eolas ag an eagraíocht agus an bhfuil sé san áireamh sa liosta foinsí?
2. An bhfuil an síniú PGP ceart?
3. I gcás amhrais, déan seiceáil ar cheanntásca iomlána teachtaireachta.
4. I gcás amhrais, úsáid “nslookup” nó “dig” chun fearann an tseoltóra a fhíorú²⁰.

WWW - Foinsí

1. Seiceáil deimhnithe brabhsálaí nuair atá nascadh á dhéanamh le láithreán gréasáin daingnithe (https ://).
2. Seiceáil an foinse maidir le hábhar agus bailíocht (theicniúil).
3. I gcás amhrais, ná cliceáil aon nasc agus ná híoslódail aon bhogearraí.
4. I gcás amhrais, déan “lookup” agus “dig” i ndáil leis an bhfearann agus déan “traceroute”.

Teileafón

1. Éist go cúramach leis an ainm.
2. An aithníonn tú an guth?
3. I gcás amhrais iarr uimhir theileafóin agus abair go nglaofaidh tú ar ais ar an duine lena mbaineann.

Fíor 10 Sampla de nós imeachta maidir le sainaithint faisnéise

Ábharthacht

Is féidir an forléargas a ullmhaíodh roimhe sin maidir le crua-earraí agus bogearraí atá suiteáilte a úsáid chun an fhaisnéis leochaileacht isteach faoi ábharthacht a scagadh d’fhonn freagra a fháil ar na ceisteanna seo a leanas: “An úsáideann an chliantacht an cineál seo bogearraí?”; “An bhfuil an fhaisnéis ábhartha dóibh?”

Aicmiú

D’fhéadfadh sé go mbeidh roinnt faisnéise a gheofar lipeadaithe mar fhaisnéis shrianta (mar shampla, tuairiscí isteach ó fhoirne eile maidir le teagmhais). Ní mór gach faisnéis a láimhseáil de réir éileamh an tseoltóra agus de réir an pholasaí dhílis maidir le slándáil fhaisnéise. Bunriail mhaith is ea “Ná scaip faisnéis mura bhfuil sé soiléir ger ceart í a scaipeadh; i gcás amhrais, faigh cead ón seoltóir chun déanamh amhlaidh.”

²⁰ Uirlisí chun céannachtaí a sheiceáil sa CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Measúnú priacal & anailísiú tionchair

Tá roinnt modhanna ann chun priacal agus tionchar leochaileachta (ionchasaí) a chinneadh.

Sainmhínítear priacal mar sheans ionchasach gur féidir an leochaileacht a dhúshaothrú. Tá roinnt gnéithe tábhachtacha ann (i measc cuid mhór acu):

- An bhfuil eolas forleathan ar an leochaileacht?
- An bhfuil an leochaileacht forleathan?
- An bhfuil sé éasca an leochaileacht a dhúshaothrú?
- An leochaileacht í atá indúshaothraithe go cianda?

Is léiriú an-mhaith na ceistanna sin go léir ar thromchúis na leochaileachta.

Tá cur chuige an-simplí chun an priacal a ríomh le fáil san fhoirmle seo a leanas:

Tionchar = Priacal X Damáiste ionchasach

D'fhéadfadh sé gurb é seo a leanas atá i ndamáiste ionchasach:

- Rochtain neamhúdairithe ar shonraí
- Seirbhís a Dhiúltú (DOS)
- Ceadanna a ghnóthú nó a leathnú

(Chun scéimeanna aicmiúcháin níos mionsonraithe a fháil, féach deireadh na caibidle seo le do thoil).

Nuair atá freagraí faighte ar na ceistanna seo is féidir rátáil fhoriomlán a chur leis an ábhar comhairleach lena ndéantar priacail ionchasacha agus damáiste ionchasach a chur in iúl. Is minic a úsáidtear téarmaí simplí ar nós ÍSEAL, MEÁNACH agus ARD.

Seo a leanas scéimeanna eile níos cuimsithí maidir le measúnú priacal:

Scéim rátála GOVCERT.NL²¹

Tá CSIRT GOVCERT.NL rialtasach na hÍsiltíre tar éis mairís a fhorbairt chun priacail a mheasúnú ar mairís í a forbraíodh ag céim tosaithe Govcert.nl agus tá sí á huasdátú fós de réir na dtreochtaí is déanaí.

²¹ Mairís leochaileachta: <http://www.govcert.nl/download.html?f=33>

RISK

Is the vulnerability widely known?	No, limited	1	Yes, public	2
Is the vulnerability widely exploited?	No	1	Yes	2
Is it easy to exploit the vulnerability?	No, hacker	1	Yes, script kiddie	2
Precondition: default configuration?	No, specific	1	Yes, standard	2
Precondition: physical access required?	Yes	1	No	2
Precondition: user account required?	Yes	1	No	2

11,12	High
8,9,10	Medium
6,7	Low

Damage

Unauthorized access to data	No	0	Yes, read	2	Yes, read +	4
DoS	No	0	Yes, non-critical	1	Yes, critical	5
Permissions	No	0	Yes, user	4	Yes, root	6

6 t/m 15	High
2 t/m 5	Medium
0,1	Low

OVERALL

High	Remote root	>> Immediately action needed!
	Local root exploit (attacker has a user account on the machine)	
	Denial of Service	
Medium	Remote user exploit	>> Action within a week
	Remote unauthorized access to data	
	Unauthorized obtaining data	
	Local unauthorized access to data	
Low	Local unauthorized obtaining user-rights	>> Include it in general process
	Local user exploit	

Fíor 11 Scéim rátála GOVCERT.NL

Cur Síos Coiteann ar Fhormáid Ábhair Chomhairligh EISPP²²

Is é atá sa Chlár Eorpach um Chur Chun Cinn Slándála Faisnéise (EISPP) ná tionscadal atá á chómhaoiniú ag an gComhphobal Eorpach faoin gCúigiú Creatchlár. Is é is aidhm do thionscadal EISPP ná creat Eorpach a fhorbairt, ní amháin chun faisnéis slándála a chomhroinnt ach freisin chun sainmhíniú a dhéanamh ar ábhar na faisnéise slándála agus ar na bealaí chun an fhaisnéis sin a scaipeadh ar SME-anna. Trí na seirbhísí slándála IT riachtanacha a sholáthar do SME-anna Eorpacha, spreagfar dóibh forbairt a dhéanamh ar a muinín i ríomhthráchtáil agus ar an úsáid a bhaineann siad as an ríomhthráchtáil, rud as a leanfadh deiseanna méadaithe agus deiseanna níos fearr do ghnóthaí nua. Tá an EISPP ina cheannródaí i dtaca le fíis an Choimisiúin Eorpaigh maidir le gréasán Eorpach oilteachta a fhoirmiú laistigh den Aontas Eorpach.

Formáid Ábhar Chomhairligh DAF Deutsche²³

Is é atá in DAF ná tionscnamh de chuid CERT-Verbund na Gearmáine agus is comhchuid lárnach é de chuid bonneagair le haghaidh ábhar comhairleach slándála a ghiniúint agus a mhalartú ag foirne éagsúla. Rinneadh DAF a shaincheapadh i gcomhair riachtanais CERT-anna na Gearmáine; tá an caighdeán á fhorbairt agus á chothabháil ag CERT-Bund, DFN-CERT, PRESECURE agus Siemens-CERT.

²² EISPP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

²³ DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

3

Beart 3: An fhaisnéis a dháileadh

Is féidir le CSIRT rogha a dhéanamh as measc roinnt modhanna dáiliúcháin, ag brath ar mhianta na gcliant agus ar do straitéis chumarsáide.

- Láithreán gréasáin
- Ríomhphost
- Tuarascálacha
- Cartlannú agus taighde

Is ceart, maidir le hábhar comhairleach slándála ó CSIRT, go mbeadh an struchtúr céanna ann i gcónaí. Sa tslí sin, feabhsófar inléiteacht agus beidh an léitheoir in ann an fhaisnéis iomchuí go léir a aimsiú go tapa.

Is ceart go mbeadh an fhaisnéis seo a leanas go léir le fáil in ábhar comhairleach:

Teideal an ábhair chomhairligh	
.....	
Uimhir thagartha	
.....	
Na córais lena mbaineann	
-	
-	
OS gaolmhar + leagan	
.....	
Priacal	(Ard-Meánach-Íseal)
.....	
Tionchar/damáiste ionchasach	(Ard-Meánach-Íseal)
.....	
ID-anna seachtracha:	(CVE, IDE-anna Feasacháin Leochaileachta)
.....	
Forléargas ar leochaileacht	
.....	
Tionchar	
.....	
Réiteach	
.....	
Cur síos (mionsonraí)	
.....	
Aguisín	
.....	

Fíor 12 Scéim shamplach le haghaidh ábhair chomhairligh

Féach caibidil 10. *Ceacht* chun sampla iomlán a fháil d'ábhar comhairleach.

8.3 Láimhseáil Teagmhas a Chur i nGníomh

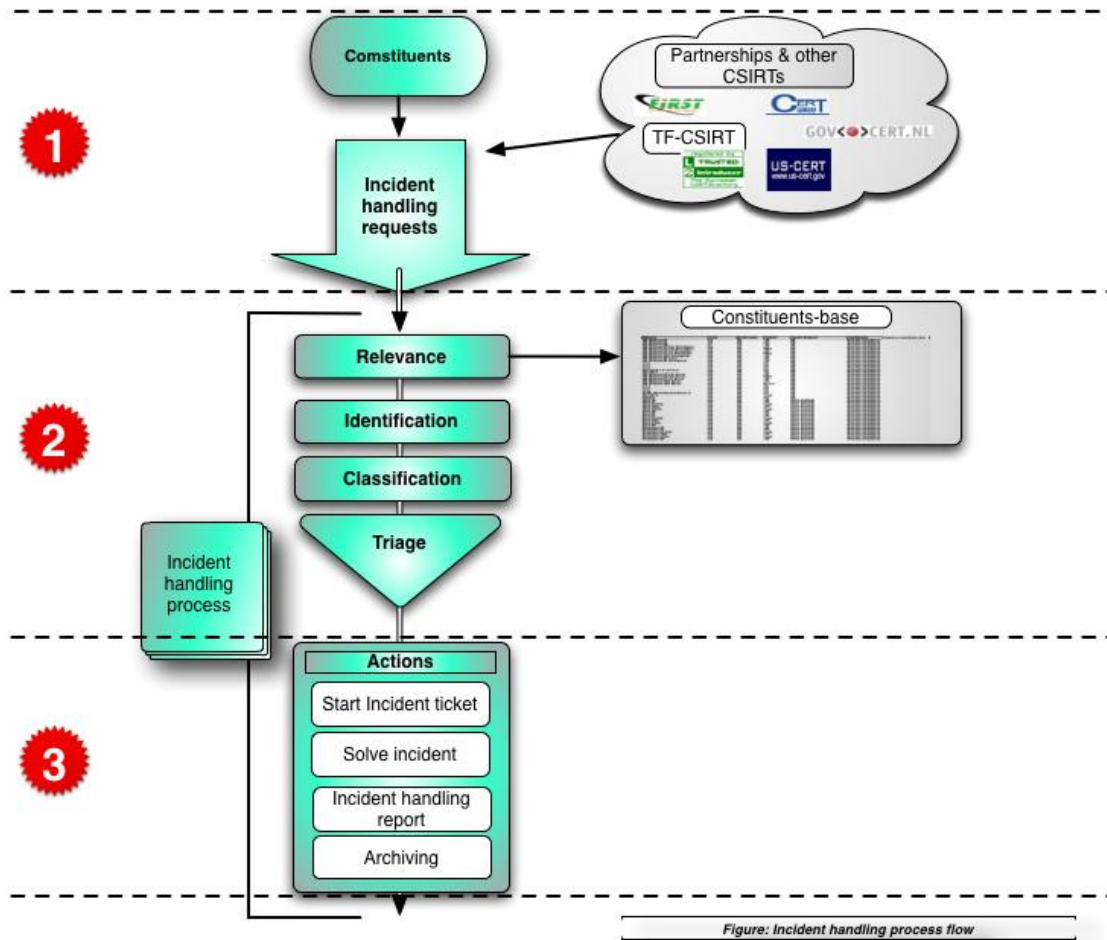
Mar atá luaite sa réamhrá a ghabhann leis an gcaibidil seo, tá an próiseas láimhseála teagmhais le linn teagmhais a láimhseáil an-chosúil leis an bpróiseas a úsáidtear nuair atá foláirimh, rabhaidh agus fógairtí á dtiomsú. Ach bíonn an chuid a bhaineann le bailiú faisnéise éagsúil de ghnáth, mar gurb é an ghnáthshlí ina bhfaightear sonraí a bhaineann le teagmhas ná trí thuairiscí teagmhais a fháil ón gcliantacht nó ó fhoirne eile, nó trí aiseolas a fháil ó pháirtithe bainteacha le linn an phróisis láimhseála teagmhais. Is gnáth faisnéis a sheoladh trí ríomhphost (criptithe); uaireanta is gá úsáid a bhaint as teileafón nó facs.

Nuair atá faisnéis á fáil le teileafón, is dea-chleachtas é gach uile mhionsonra a nótáil trí leas a bhaint as uirlis láimhseála/tuairiscithe teagmhais nó trí mheamram a dhéanamh. Is gá (roimh dheireadh an ghlaigh) uimhir theagmhais a ghiniúint láithreach (mura bhfuil aon uimhir ann cheana féin don teagmhas lena mbaineann) agus an uimhir sin a eisiúint chuig an tuairisceoir teileafóin (nó trí theachtaireacht achomair ríomhphoist tar eis an ghlaigh) agus sin a dhéanamh mar ábhar tagartha i gcomhair cumarsáidí ina dhiaidh sin.

Sa chuid eile den chaibidil seo, déantar cur síos ar an mbunphróiseas a bhaineann le láimhseáil teagmhais. Is féidir anailís an-leathan ar an bpróiseas iomlán a bhaineann le bainistiú teagmhas agus ar an sreabhadh oibre agus ar an bhfoshreabhadh oibre lena mbaineann a fháil i ndoiciméad de chuid CERT/CC dar teideal *Defining Incident Management processes for CSIRTs*²⁴.

²⁴ Próisis Bhainistíochta Teagmhas a Shainmhíniú: <http://www.cert.org/archive/pdf/04tr015.pdf>

Go bunúsach, leanann láimhseáil teagmhas an sreabhadh oibre seo a leanas:



Fíor 13 Sreabhadh oibre an phróisis

1**Beart 1: Tuairiscí a fháil faoi theagmhais**

Mar atá luaite roimhe seo, sroicheann tuairiscí faoi theagmhais CSIRT trí bhealaí éagsúla, go háirithe le ríomhphost ach freisin le teileafón nó le facs.

Mar atá luaite roimhe seo, is dea-chleachtas é na mionsonraí go léir a nótaíl i bhformáid sheasta le linn glacadh le tuairisc faoi theagmhas. Sa tslí sin, cinntítear nach bhfágтар aon fhaisnéis fhíorthábhachtach ar lár. Ina dhiaidh sin, is féidir scéim shamplach a aimsiú:

FOIRM THUAIRISCITHE TEAGMHAIS

*Comhlánaigh an fhoirm seo le do thoil agus seol í le Facs nó le ríomhphost chuig:
Tá an fhaisnéis a iarrtar ar línte lena ngabhann * éigeantach.*

Ainm na hEagraíochta

1. Ainm*:
2. Ainm na hEagraíochta*:
3. An cineál earnála:
4. Tír*:
5. Cathair:
6. Seoladh ríomhphoist*:
7. Uimhir theileafóin*:
8. Eile:

Óstach(Óstaigh) lena mbaineann

9. An líon óstach:
10. Ainm an óstaigh & IP*:
11. Feidhm an Óstaigh*:
12. An Réigiún Ama:
13. Crua-earra:
14. Córas Oibríochta:
15. Bogearraí lena mbaineann:
16. Comhaid lena mbaineann:
17. Slándáil:
18. Ainm an Óstaigh & IP:
19. Prótacal/port:

Teagmhas

20. Uimhir thagartha # thag.:
21. An cineál teagmhais:
22. Dáta tosaigh an teagmhais:
23. An teagmhas leanúnach é seo:: SEA NÍ hEA
24. Am agus modh fionnachtana:
25. Leochaileachtaí atá ar eolas:
26. Comhaid Amhrasacha:
27. Frithbhearta:
28. Cur síos mionsonraithe*:

Fíor 14 Ábhar tuairisce faoi theagmhas

2

Beart 2: Teagmhas a mheasúnú

Le linn an bhirt seo, déantar fíre agus ábharthacht teagmhais thuairiscithe a sheiceáil agus aicmítear an teagmhas.

Sainaithint

Chun aon ghníomh gan ghá a sheachaint is níosmháireacht mhaith í seiceáil a dhéanamh i dtaobh an bhfuil an tionscnóir iontaofa agus an bhfuil an tionscnóir i measc do chuid cliant nó i measc chliant CSIRT ghaolmhair de do chuid. Tá feidhm ag rialacha comhchosúla de réir mar a thuairiscítear i gcaibidil 8.2 *Foláirimh a Ghiniúint*.

Ábharthacht

Tríd an mbeart seo, déanann tú seiceáil i dtaobh an dtagann an iarraidh ar laimhseáil teagmhais ó chliantacht an CSIRT, nó am mbaineann an teagmhas a tuairiscíodh leis an gcliantacht. Más rud é nach mbaineann ceachtar de na nithe thuas le hábhar, déantar an tuairisc a atreorú de ghnáth chuig an CSIRT ceart²⁵.

Aicmiú

Tríd an mbeart seo, déantar an triáis a ullmhú trí dhéine an teagmhais a aicmiú. Tá sé lasmuigh de scóip an doiciméid seo mionsonraí a thabhairt maidir le haicmiú teagmhais. Tús maith is ea úsáid a bhaint as scéim Aicmithe Cáis CSIRT (Sampla do CSIRT Fiontair):

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	DOS or DDOS attack.
Forensics	S1	Any forensic work to be done by CSIRT.
Compromised Information	S1	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	- Sharing offensive material, sharing/possession of copyright material. - Deliberate violation of Infosec policy. - Inappropriate use of corporate asset such as computer, network, or application. - Unauthorized escalation of privileges or deliberate attempt to subvert access controls.

* - Sensitivity will vary depending on circumstances. Guidelines are provided.

Fíor 15 Scéim aicmithe teagmhas (foinse: FIRST)²⁶

²⁵ Uirlisí chun céannachtaí a sheiceáil sa CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

²⁶ Aicmiú Cáis CSIRT http://www.first.org/resources/guides/csirt_case_classification.html

Triáis

Is é atá i dtriáis ná córas a úsáideann pearsanra liachta nó éigeandála chun acmhainní teoranta liachta a chiondáil nuair is mó an líon daoine gortaithe ná na hacmhainní atá ar fáil chun cúram a thabhairt ionas gur féidir cóireáil a thabhairt don líon is mó othar is féidir²⁷.

Tugtar an cur síos seo a leanas sa CERT/CC:

Tá triáis ina ghné riachtanach d'aon chumas bainistithe teagmhais, go háirithe i gcomhair CSIRT seanbhunaithe. Baineann triáis leis an gconair chriticiúil i gcomhair tuiscint a fháil ar cad atá á thuairisciú ar fud na heagraíochta. Fónann sé mar fheithicil ar tríthi a shníonn an fhaisnéis go léir isteach i bpointe teagmhála aonair, rud a fhágann gur féidir léargas forleathan a fháil ar ghníomhaíocht leanúnach agus gur féidir comhghaolú cuimsitheach a dhéanamh ar na sonraí go léir a thuairiscítear. Ceadaíonn triáis measúnú inmheánach a dhéanamh ar thuairisc isteach agus cuireann sé i scuaine é lena láimhseáil ina dhiaidh sin. Ina theannta sin, soláthraíonn sé ionad chun tús a chur le doiciméadú tosaigh agus le hiontráil sonraí maidir le tuairisc nó iarraidh, i gcás nach ndearnadh amhlaidh sa phróiseas Braite.

Leis an fheidhm thríaise, soláthraítear pictiúr láithreach den stádas reatha i ndáil le gach gníomhaíocht atá tuairiscithe — cé na tuairiscithe atá oscailte nó dúnta, cé na gníomhartha atá ar feitheamh, agus cá mhéad tuairiscí de gach cineál atá faighte. Is féidir leis an bpróiseas seo a bheith ina chabhair maidir le fadhbanna ionchasacha slándála a shainaithint agus maidir le tosaíochtaí a dhéanamh i dtaca leis an ualach oibre. Is féidir faisnéis a bhailítear le linn triáise a úsáid freisin chun treochtaí leochaileachta agus teagmhais, mar aon le staitisticí ina leith sin, a ghiniúint don lucht bainistíochta sinsearach²⁸.

Triage should only be done by the most experienced team members, because it requires deep understanding of the potential impacts of incidents on specific parts of the constituency and the ability to decide who would be the appropriate team member to handle that incident.

²⁷ Triáis in Wikipedia: <http://en.wikipedia.org/wiki/Triage>

²⁸ Próisis Bhainistithe Teagmhas a Shainmhíniú: <http://www.cert.org/archive/pdf/04tr015.pdf>

3

Beart 3: Gníomhartha

De ghnáth, téann teagmhais triáisithe isteach i scuaine iarrataí in uirlis láimhseála teagmhas a úsáideann láimhseálaí amháin nó níos mó a leanann na bearta seo a leanas go bunúsach.

Tús a chur le ticéad teagmhais

D'fhéadfadh sé go mbeifear tar éis uimhir an ticéid teagmhais a ghiniúint cheana féin (mar shampla, nuair a tuairiscíodh an teagmhas le teileafón). Mura bhfuil a leithéid ann, is é atá sa chéad chéim ná an uimhir sin a chruthú agus úsáidfear í i ngach cumarsáid ina dhiaidh sin maidir leis an teagmhas céanna.

Saolré teagmhais

I gcás teagmhas a láimhseáil, ní leantar sraith beart as a dtagann réiteach deiridh, ach leantar ciorcal beart a chuirtear i bhfeidhm arís agus arís eile go dtí go réitítear an teagmhas sa deireadh agus go bhfuil an fhaisnéis riachtanach go léir ag na oárithe go léir lena mbaineann. Tá na próisis seo a leanas san áireamh sa chiorcal sin ar a dtugtar “An Saolré Teagmhais” go minic freisin:

<i>Anailís:</i>	Déantar gach mionsonra faoin teagmhas tuairiscithe a anailísiú.
<i>Faisnéis teagmhála a fháil:</i>	Chun bheith in ann faisnéis a thuairisciú tuilleadh faoin teagmhas do na páirtithe go léir lena mbaineann, ar nós CSIRT-anna eile, íospartaigh agus, is dócha, úinéirí córas a bhféadfaí mí-úsáid a bheith bainte astú i ndáil le hionsaí.
<i>Cúnamh teicniúil a sholáthar:</i>	Cabhrú le híospartaigh téarnamh a dhéanamh go tapa tar éis an teagmhais agus tuilleadh faisnéise a bhailiú faoin ionsaí.
<i>Comhordú:</i>	Eolas a chur in iúl do pháirtithe eile lena mbaineann, mar shampla an CSIRT atá freagrach as an gcóras IT a úsáideadh le haghaidh ionsaí, nó íospartaigh eile.

Tugtar “saolré” ar an struchtúr seo mar go leanann beart eile agus an beart deireanach as ceann de na bearta, is é sin le rá an beart comhordaithe agus mar go bhféadfadh anailís nua a bheith ag teastáil agus, dá bhrí sin, go gcuirfí tús leis an timthriall athuair. Tagann deireadh leis an bpróiseas nuair a fhaigheann agus nuair a thuairiscíonn na páirtithe go léir lena mbaineann an fhaisnéis riachtanach go léir.

Féach lámhleabhar CERT/CC CSIRT le do thoil chun cur síos níos mionsonraithe a fháil ar an saolré teagmhais²⁹.

Tuairisc láimhseála teagmhais

Bí ullamh chun ceisteanna maidir le teagmhais ón lucht bainistíochta a fhreagairt trí thuairisc a thiomsú. Is dea-chleachtas é freisin doiciméad a scríobh faoi “ceachtanna a foghlaimíodh” (lena úsáid go himheánach amháin) mar ábhar teagaisc don fhoireann

²⁹ Lámhleabhar CSIRT: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

agus chun botúin a sheachaint sa todhchaí maidir le próisis láimhseála teagmhas.

Cartlannú

Déan staidéar ar na rialacha a bhaineann le cartlannú agus a thuairiscítear níos túisce i gcaibidil 6.6 *Polasaí slándála faisnéise a fhorbairt*.

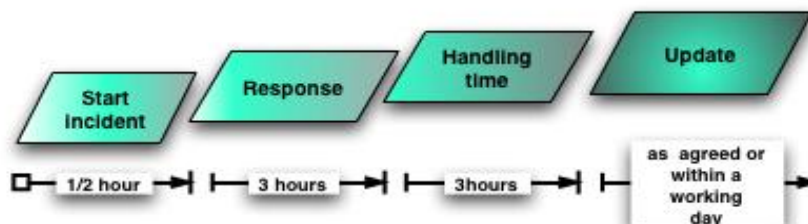
Féach roinn A den Aguisín, le do thoil, *A.1 Tuilleadh ábhair leitheoireachta* chun treoracha cuimsitheacha a fháil maidir le bainistiú teagmhas agus saolré teagmhas.

8.4 Sampla d'amchlár freagartha

Is minic a dhéantar neamhshuim d'amanna freagartha ach ní mór é sin a bheith ina chuid de gach comhaontú dea-struchtúrtha leibhéil seirbhíse (SLA) idir CSIRT agus a chliantacht. Tá sé thar a bheith tábhachtach go dtabharfaí aiseolas tráthúil do chliant le linn teagmhas a láimhseáil, i dtaca le dlíteanais na gcliant féin de agus i dtaca le clú na foirme de.

Ní mór na hamanna freagartha a chur in iúl go soiléir don chliantacht le nach mbeifear ag súil le nithe nach dtarlóidh. Is féidir an t-amchlár an-bhunúsach seo a leanas a úsáid mar phointe tosaigh i gcomhair SLA níos mionsonraithe le cliantacht CSIRT.

Seo a leanas sampla d'amchlár praiticiúil freagartha agus é bunaithe ar iarraidh isteach ar chúnamh:



Fíor 16 Sampla d'amchlár freagartha

Is dea-chleachtas é freisin treoir a thabhairt don chliantacht maidir lena n-amanna freagartha féin, go háirithe maidir le cathain is ceart teagmháil a dhéanamh leis an CSIRT i gcás éigeandála. Sa chuid is mó cásanna is fearr teagmháil a dhéanamh leis an CSIRT go luath agus is dea-chleachtas é spreagadh a thabhairt don chliantacht déanamh amhlaidh i gcás amhras a bheith ann.

8.5 Uirlisiú CSIRT atá ar fáil

Sa chaibidil seo, soláthraítear roinnt eolais faoi uirlisí coitianta a úsáideann CSIRT-anna. Níl ann ach samplaí agus is féidir eolas eile a fháil in *Clearinghouse of Incident Handling Tools*³⁰ (CHIHT).

Bogearraí criptithe ríomhphoist agus teachtaireachtaí

- GNUPG <http://www.gnupg.org/>
Is é atá in GnuPG ná cur i bhfeidhm iomlán, saor in aisce thionscadal GNU i dtaca le caighdeán OpenPGP mar a shainmhínítear le RFC2440. GnuPG trína gceadaítear duit do chuid sonraí agus cumarsáidí a chriptiú agus a shíniú.
- PGP <http://www.pgp.com/>
Malairt tráchtála

Uirlis láimhseála teagmhas

Riaradh teagmhas agus gníomhartha tar éis teagmhais do tharlú, bearta a rianú.

- RTIR <http://www.bestpractical.com/rtir/>
Is é atá in RTIR ná córas saor in aisce foinse oscailte maidir le láimhseáil teagmhas ar córas é atá ceaptha i gcomhair riachtanais fhoirne CSIRT agus foirne eile freagartha teagmhas.

Uirlisí CRM

Nuair atá cuid mhór cliant éagsúil agat agus nuair is gá gach coinne agus gach mionsonra a rianú, tá bunachar sonraí CRM cuiditheach. Tá a lán malairtí éagsúla ann; seo a leanas roinnt samplaí:

- SugarCRM <http://www.sugarcrm.com/crm/>
- Sugarforce (Leagan saor in aisce foinse oscailte) <http://www.sugarforge.org/>

Seiceáil faisnéise

- Website watcher <http://www.aignes.com/index.htm>
Déanann an ríomhchlár seo faireachán ar láithreáin ghréasáin chun teacht ar ábhar uasdátaithe agus ar athruithe.
- Watch that page <http://www.watchthatpage.com/>
Cuireann an tseirbhís seo faisnéis le ríomhphost i ndáil le hathruithe ar láithreáin ghréasáin (seirbhís atá ar fáil saor in aisce agus ar bhonn tráchtála).

³⁰ CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Faisnéis teagmhála a aimsiú

Ní bhíonn sé éasca teacht ar na sonraí cearta teagmhála chun teagmhais a thuairisciú. Tá cúpla foinse faisnéise ar fáil lena n-úsáid:

- RIPE³¹
- IRT-object³²
- TI³³

Ina theannta sin, tá roinnt uirlisí chun teacht ar fhaisnéis liostaithe ag CHIHT³⁴.

CSIRT samhailteach (beart 8)

Sreabhadh próisis agus nósanna imeachta oibríochta agus teicniúla a bhunú

Díríonn CSIRT samhailteach ar sheirbhísí lárnacha a sholáthar:

- Foláirimh agus Rabhaidh
- Fógairtí
- Láimhseáil Teagmhas

D'fhorbair an fhoireann nósanna imeachta a oibríonn go maith agus atá sothuigte ag gach ball foirne. D'earcaigh an CSIRT samhailteach saineolaí dlí freisin chun déileáil le dliteanais agus leis an bpolasaí maidir le slándáil fhaisnéise. Ghlac an fhoireann roinnt uirlisí úsáideacha agus d'aimsigh siad faisnéis chuiditheach faoi shaincheisteanna oibríochta trí phlé a dhéanamh le CSIRT-anna eile.

Gineadh teimpléad seasta le haghaidh ábhar comhairleach maidir le slándáil agus le haghaidh tuairiscí faoi theagmhais. Úsáideann an fhoireann RTIR chun teagmhais a láimhseáil.

³¹ RIPE whois: <http://www.ripe.net/whois>

³² Oibiacht IRT i mbunachar sonraí RIPE: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

³³ Tionscnóir iontaofa: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

³⁴ Uirlisí chun céannachtaí in CHIHT a sheiceáil: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9. Oiliúint CSIRT

Tá na bearta seo a leanas déanta againn go dtí seo:

1. Tuiscint a fháil ar céard é CSIRT agus cé na tairbhí a d'fhéadfadh a bheith ann dá bharr.
2. Cén earnáil a soláthróidh an fhoireann nua a cuid seirbhísí di?
3. Cad iad na cineálacha seirbhísí atá CSIRT in ann a sholáthar dá chliantacht.
4. Anailís a dhéanamh ar an timpeallacht agus ar na cliaint.
5. An ráiteas misin a shainmhíniú.
6. An Plean Gnó a Fhorbairt.
 - a. An múnla airgeadais a shainmhíniú.
 - b. An múnla eagrúcháin a shainmhíniú.
 - c. Tús a chur le hearcú foirne.
 - d. Úsáid agus trealmhú na hoifige.
 - e. Polasaí slándála faisnéise a fhorbairt
 - f. Comhpháirtithe comhoibrithe a chuardach.
7. An Plean Gnó a Chur Chun Cinn.
 - a. Ceadú a fháil don chás gnó.
 - b. Gach rud a chur isteach i bplean tionscadail.
8. An CSIRT a chur i bhfeidhm.
 - a. Sreabhadh oibre a chruthú
 - b. Uirlisiú CSIRT a chur i ngníomh

>> Is é atá sa chéad bheart eile ná an fhoireann a oiliúint

Sa chaibidil seo, liostaítear an dá phríomhfhoinsí i gcomhair shainoiliúint CSIRT: TRANSITS agus cúrsaí CERT/CC.

9.1 TRANSITS

Is é a bhí in TRANSITS ná tionscadal Eorpach chun bunú Foirne Freagartha Teagmhas Slándála Ríomhaire (CSIRT-anna) a chur chun cinn agus chun feabhas a chur ar CSIRT-anna láithreacha trí aghaidh a thabhairt ar an bhfadhb a ghabhann le ganntanas ball oile foirne CSIRT. Tugadh aghaidh ar an aidhm sin trí shainchúrsaí oiliúna a sholáthar chun baill foirne CSIRT-anna (nua) a oiliúint i ndáil le saincheistanna eagrúcháin, oibríochta, teicniúla, margaigh agus dlí a bhaineann le seirbhísí CSIRT.

Go háirithe, is é atá déanta trí TRANSITS ná:

- ábhar cúrsaí oiliúna modúlacha a fhorbairt, a uasdátú agus a athbhreithniú go tráthrialta
- ceardlanna oiliúna a eagrú ar lena linn a úsáideadh na hábhair chúrsa
- a chumasú do bhaill foirne CSIRT-anna (nua) páirt a ghlacadh sna ceardlanna oiliúna sin, agus béim ar leith ar páirteachas daoine as Stáit Aontachais AE

- ábhair chúrsaí oiliúna a scaipeadh agus a chinntiú go saothraítear torthaí na gcúrsaí³⁵.

Déanann ENISA éascaíocht maidir le cúrsaí TRANSITS agus tacaíonn sé leo. Más mian leat tuilleadh faisnéise a fháil i dtaobh conas iarratas a dhéanamh ar chúrsa, i dtaobh na gceanglas agus i dtaobh na gcostas, déan teagmháil le saineolaithe ENISA i réimse na CSIRT-anna, le do thoil:

cert-relation@enisa.europa.eu

Gheobhaidh tú ábhar sampla cúrsa san iarscríbhinn a ghabhann leis an doiciméad seo!

9.2 CERT/CC

Mar gheall ar chastacht bonneagar ríomhairí agus gréasán agus mar gheall ar am dúshlán a ghabhann le riarachán, is deacair slándáil ghréasáin a bhainistiú i gceart. Ní bhíonn dóthain daoine ná cleachtas slándála ag riarthóirí gréasán agus córas chun cosaint a dhéanamh ar ionsaithe agus chun damáiste an íoslaghdú. Dá bharr sin, tá líon méadaitheach teagmhas slándála ríomhaire ann.

Nuair a tharlaíonn teagmhais slándála ríomhaire ní mór d'eagraíochtaí gníomhú go tapa agus go héifeachtach. Má dhéanann eagraíocht teagmhas a shainaithint agus a anailísiú go tapa, agus má ghníomhaíonn sí go tapa ina leith, is amhlaidh is fearr is féidir léi damáiste a theorannú agus costais téarnaimh a laghdú. Is ionann bunú foirne freagartha teagmhas slándála ríomhaire (CSIRT) agus bealach sármhaith chun cumas freagartha thapa a sholáthar agus, freisin, chun cabhair a thabhairt maidir le teagmhais a chosc sa todhchaí.

Tairgeann CERT-CC cúrsaí do bhainisteoirí agus do phearsanra teicniúil i réimsí ar nós foirne freagartha teagmhas slándála ríomhaire (CSIRT-anna) a bhunú, gníomhú nuair a tharlaíonn teagmhais slándála agus anailís a dhéanamh orthu, agus feabhas a chur ar shlándáil ghréasán. Muar luaitear a mhalairt, seoltar na cúrsaí go léir in Pittsburgh, PA. Déanann baill dár bhfoireann cúrsaí a mhúineadh in Ollscoil Carnegie Mellon freisin.

Na Cúrsaí CERT/CC atá ar fáil³⁶ agus iad saindírithe ar CSIRT-anna

[Foireann Freagartha Teagmhas Slándála Ríomhaire \(CSIRT\) a chruthú](#)

[Foirne Freagartha Teagmhas Slándála Ríomhaire \(CSIRT-anna\) a Bhainistiú](#)

[Buneolas maidir le Láimhseáil Teagmhas](#)

[Láimhseáil Ardleibhéil Teagmhas d'Fhoireann Theicniúil](#)

Gheobhaidh tú ábhar samplach cúrsa san iarscríbhinn a ghabhann leis an doiciméad seo!

³⁵ TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

³⁶ Cúrsaí CERT/CC: <http://www.sei.cmu.edu/products/courses>



CSIRT samhailteach (beart 9)

An fhoireann a oiliúint

Déanann an CSIRT samhailteach cinneadh chun gach duine dá fhoireann theicniúil a chur ar an gcéad chúrsa TRANSITS eile atá ar fáil. Ina theannta sin, freastalaíonn ceannaire na foirne cúrsa CERT/CC dar teideal *Managing a CSIRT*.

10. Ceacht: ábhar comhairleach a ullmhú

Tá na bearta seo a leanas déanta againn go dtí seo:

1. Tuiscint a fháil ar céard é CSIRT agus cé na tairbhí a d'fhéadfadh a bheith ann dá bharr.
2. Cén earnáil a soláthróidh an fhoireann nua a cuid seirbhísí di?
3. Cad iad na cineálacha seirbhísí atá CSIRT in ann a sholáthar dá chliantacht.
4. Anailís a dhéanamh ar an timpeallacht agus ar na cliaint.
5. An ráiteas misin a shainmhíniú.
6. An Plean Gnó a Fhorbairt.
 - a. An múnla airgeadais a shainmhíniú
 - b. An múnla eagrúcháin a shainmhíniú
 - c. Tús a chur le hearcú foirne
 - d. Úsáid agus trealmhú na hoifige
 - e. Polasaí slándála faisnéise a fhorbairt
 - f. Comhpháirtithe comhoibrithe a chuardach.
7. An Plean Gnó a Chur Chun Cinn.
 - a. Ceadú a fháil don chás gnó.
 - b. Gach rud a chur isteach i bplean tionscadail.
8. An CSIRT a chur i bhfeidhm.
 - a. Sreabhadh oibre a chruthú
 - b. Uirlisiú CSIRT a chur i ngníomh
9. An fhoireann a oiliúint

>> Is é atá sa chéad bheart eile ná ceacht a dhéanamh agus ullmhúchán a dhéanamh le haghaidh na fóir-oibre!

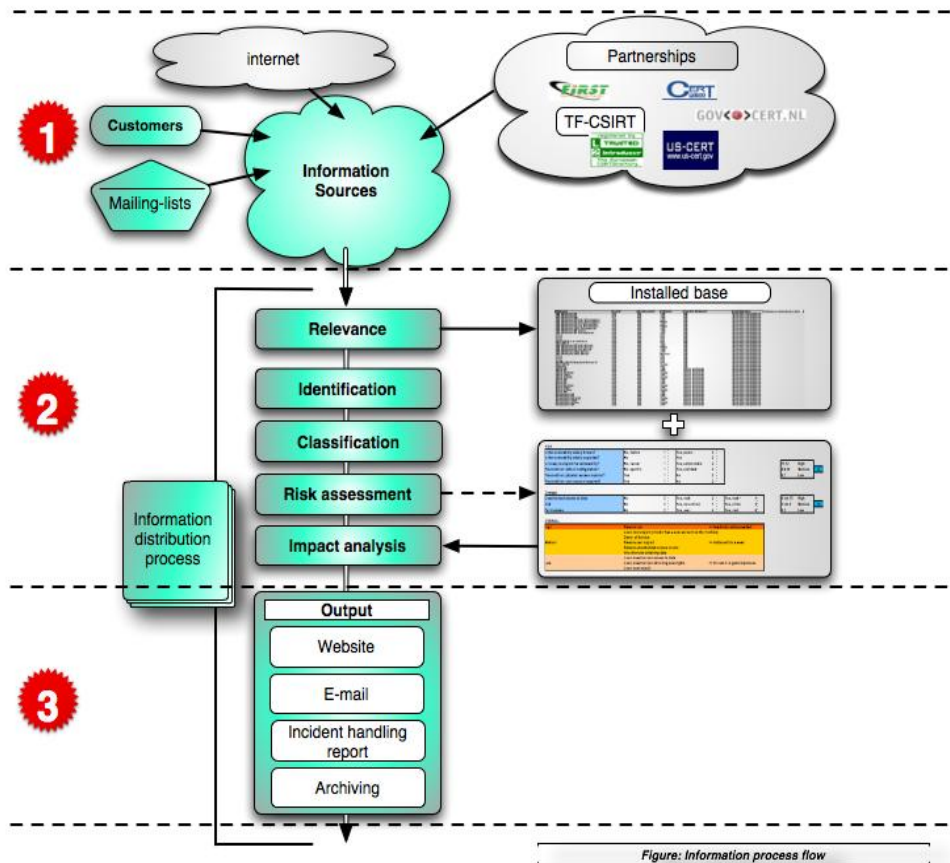
Mar léiriú, tugtar cur síos sa chaibidil seo ar cheacht i gcomhair thasc coitianta CSIRT: ábhar comhairleach a ullmhú.

Ba é a bhí sa truícear ná an t-ábhar comhairleach bunaidh seo a leanas arna eisiúint ag Microsoft:

Bulletin Identifier	Microsoft Security Bulletin MS06-042
Bulletin Title	Cumulative Security Update for Internet Explorer (918899)
Executive Summary	This update resolves several vulnerabilities in Internet Explorer that could allow remote code execution.
Maximum Severity Rating	Critical
Impact of Vulnerability	Remote Code Execution
Affected Software	Windows, Internet Explorer. For more information, see the Affected Software and Download Locations section.

San fheasachán díoltóra seo, tugtar aghaidh ar leochaileacht a aimsíodh le déanaí in Internet Explorer. Foilsíonn an díoltóir réitigh iolracha le haghaidh na mbogearraí seo i gcomhair leaganacha iolracha de Microsoft Windows.

Tar éis don CSIRT samhailteach an fhaisnéis leochaileachta seo a fháil le ríomhphost, cuireann sé tús leis an sreabhadh oibre a thuairiscítear i gcaibidil 8.2 *Foláirimh, Rabhaidh agus Fógairtí a Ghiniúint*.



1

Beart 1: Faisnéis leochaileachta a bhailiú.

Is é atá sa chéad bheart ná brabhsáil a dhéanamh chuig láithreán gréasáin an díoltóra. Déanann an CSIRT samhailteach fíre na faisnéise a fhíorú ansin agus bailíonn sé tuilleadh mionsonraí faoin leochaileacht agus faoi na córais IT lena mbaineann.

2**Beart 2: An fhaisnéis a mheasúnú agus an priacal a mheas****Sainaithint**

Rinneadh an fhaisnéis a fhíorú cheana féin tríd an bhfaisnéis leochaileachta a fuarthas le ríomhphost a chros-seiceáil in aghaidh an téacs ar láithreán gréasáin an díoltóra.

Ábharthacht

Déanann an CSIRT samhailteach an liosta córas lena mbaineann a fuarthas ar an láithreán gréasáin a sheiceáil in aghaidh an liosta córas a úsáidtear sa chliantacht. Faigheann sé amach go bhfuil Internet Explorer á úsáid ag comhchuid amháin ar a laghad agus, dá bhrí sin, is cinnte go bhfuil an fhaisnéis leochaileachta ábhartha.

Catagóir	Feidhmiúchán	Táirge bogearraí	Leagan	OS	Leagan den OS	Comhchuid
Deasc	Brabhsálaí	IE	x-x-	Microsoft	XP-prof	A

Aicmiú

Faisnéis phoiblí atá ann agus, dá bhrí sin, is féidir í a úsáid agus a athdháileadh.

An priacal a mheas & an tionchar a anailísiú

Trí na ceisteanna a fhreagairt taispeánfar go bhfuil tionchar an phriacail *ard* (arna rátáil mar phriacal *criticiúil* ag Microsoft).

PRIACAL

An bhfuil eolas maith ar an leochaileacht?	Tá
An bhfuil an leochaileacht forleathan?	Tá
An bhfuil sé éasca an leochaileacht a dhúshaothrú?	Tá
An bhfuil an leochaileacht indúshaothraithe go cianda?	Tá

DAMÁISTE

Tionchair ionchasacha is ea rochtain chianda agus forghníomhú ionchasach cóid go cianda. Tá saincheisteanna iolracha ann maidir leis an leochaileacht seo, rud a fhágann go bhfuil leibhéal an phriacail go ndéanfar damáiste *ard*.



Beart 3: Dáileadh

CSIRT inmheánach atá sa CSIRT samhailteach. Tá ríomhphost, fón agus an láithreán gréasáin inmheánach ar fáil aige mar bhealaí cumarsáide. Ullmhaíonn an CSIRT an t-ábhar comhairleach seo a leanas, agus é bunaithe ar an teimpléad i gcaibidil 8.2 *Foláirimh, Rabhaidh agus Fógairtí a Ghiniúint*.

Teideal an Ábhair Chomhairligh

Leochaileachtaí iolracha faighte in Internet explorer

Uimhir thagartha

082006-1

Na córais lena mbaineann

Gach córas deisce a ritheann Microsoft

OS gaolmhar + leagan

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

Priacal

(Ard-Meánach-Íseal)

ARD

Tionchar/damáiste ionchasach

(Ard-Meánach-Íseal)

ARD

ID-anna seachtracha:

(CVE, ID-anna Feasacháin Leochaileachta)

MS-06-42

Forléargas ar an leochaileacht

Tá roinnt leochaileachtaí criticiúla aimsithe ag Microsoft in Internet Explorer ar leochaileachtaí iad a bhféadfadh forghníomhú cóid cianda leanúint astu.

Tionchar

D'fhéadfadh ionsaitheoir rialú iomlán a fháil ar an gcóras agus ríomhchláir a shuiteáil, úsáideoirí a chur leis agus sonraí a bhreathnú, a athrú nó a scríosadh. Gné mhaolaitheach is ea nach féidir go dtarlódh an méid sin thuas ach amháin má bhíonn an t-úsáideoir logáilte isteach le cearta riarthóra. D'fhéadfadh tionchar níos lú a bheith ann i gcás úsáideoirí atá logáilte isteach gan cearta riarthóra.

Réiteach

An IE a phaitseáil laithreach

Cur síos (mionsonraí)

Féach tuilleadh faisnéise [ms06-042.msp](https://msrc.microsoft.com/updatecatalogs/ms06-042/ms06-042.msp)

Aguisín

Féach tuilleadh faisnéise [ms06-042.msp](https://msrc.microsoft.com/updatecatalogs/ms06-042/ms06-042.msp)

Tá an t-aschur seo réidh lena dháileadh anois. Ó tharla gur feasachán criticiúil é, tá sé inmhianaithe glaoch a chur ar na cliaint freisin más féidir sin.

CSIRT samhailteach (beart 10)**Ceacht a dhéanamh**

Le linn chéad seachtainí na n-oibríochtaí, úsáideann an CSIRT samhailteach roinnt cásanna samhailteacha (a fuarthas mar shamplaí ó CSIRT-anna eile) a úsáideadh mar cheacht. Ina theannta sin, d'eisigh siad ábhar áirithe comhairleach a bhí bunaithe ar fhíorfhaisnéis leochaileachta arna dáileadh ag díoltóirí crua-earraí agus bogearraí ar ábhar é a athraíodh agus a oiriúnaíodh de réir riachtanais na cliantachta.

11. Conclúid

Seo deireadh na treorach. Tá an doiciméad seo beartaithe chun forléargas an-achomair a thabhairt ar na próisis atá riachtanach chun CSIRT a chur ar bun. Ní mhaítear gur treoir iomlán í ná ní thugtar an iomarca mionsonraí. Léigh an roinn dar teideal *A.1 Tuilleadh ábhair léitheoireachta* san iarscríbhinn chun ábhar a fháil faoin topaic is díol spéise duit.

Is é atá sna chéad bhearta tábhachtacha eile do CSIRT samhailteach ná:

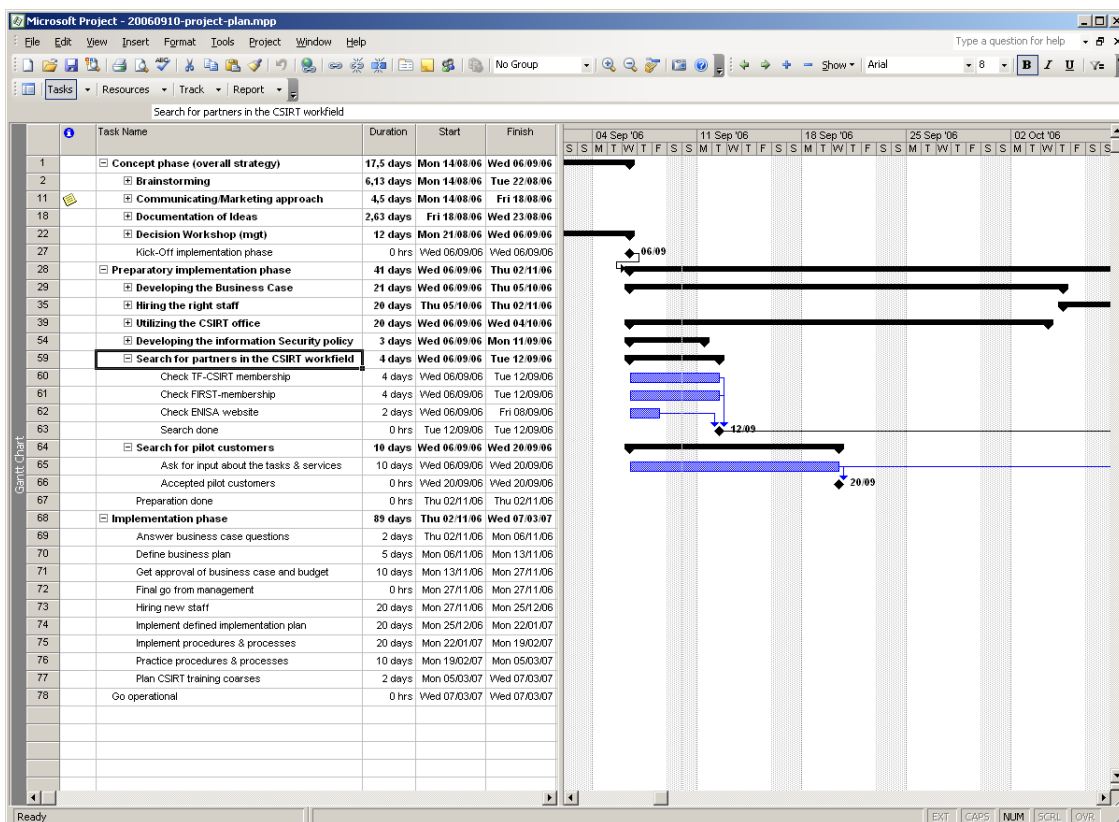
- Aiseolas a fháil ón gcliantacht chun na seirbhísí a sholáthraítear a oiriúnú tuilleadh
- Gnáthamh a bhunú san obair ó lá go lá
- Staideanna éigeandála a chur i bhfeidhm
- Dlúth-theagmháil a choimeád ar bun leis na comhphobail éagsúla CSIRT d'fhonn cabhair a thabhairt dá gcuid oibre saorálai lá éigin

12. Cur síos ar Phlean Tionscadail

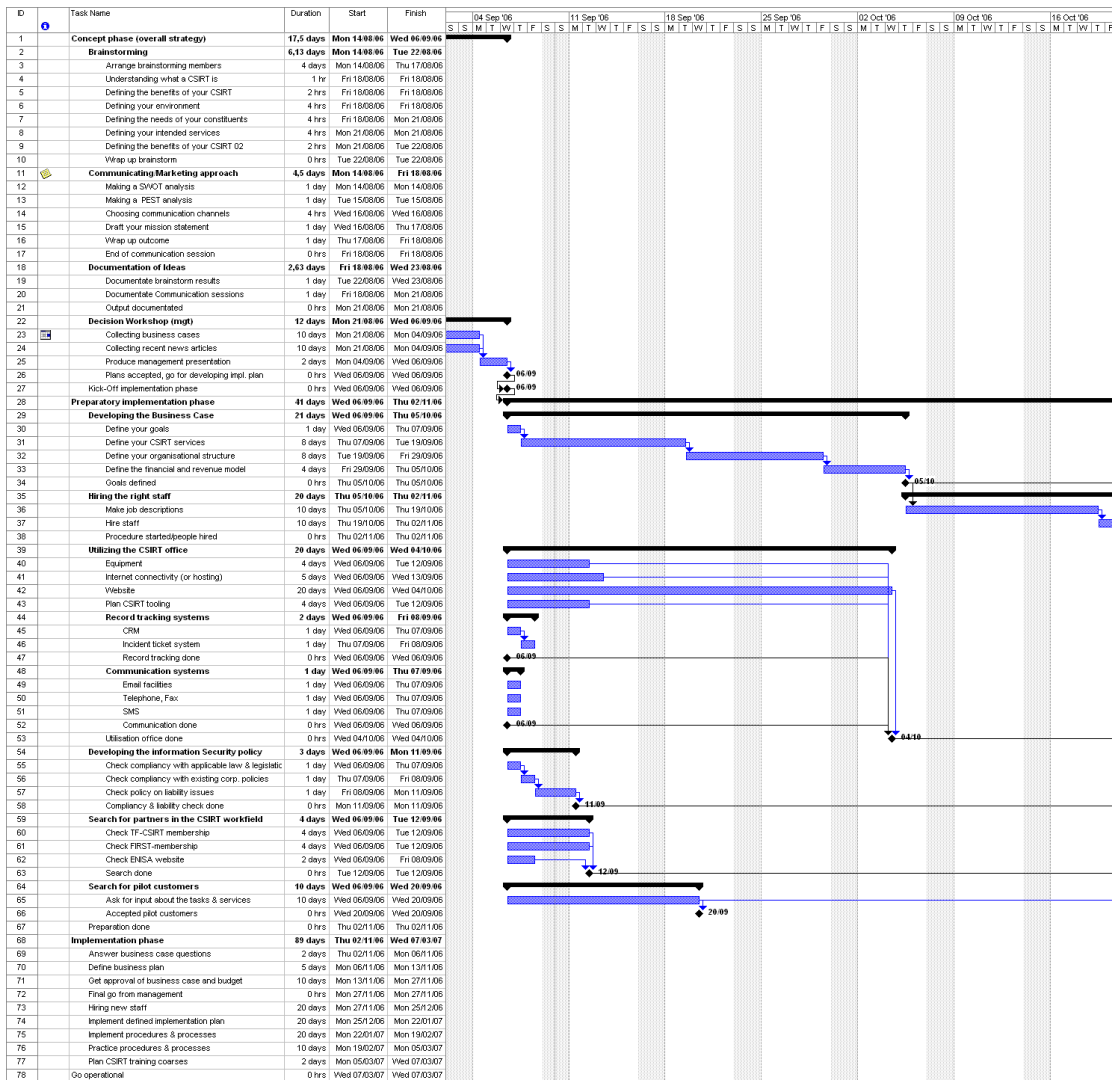
NÓTA: Is é atá sa phlean tionscadail ná an chéad mheastachán ar an am atá ag teastáil. Ag brath ar na hacmhainní atá ar fáil, d'fhéadfadh sé tarlú nach mbeidh fíorfhad an tionscadail mar an gcéanna.

Tá an plean tionscadail ar fáil i bhformáidí éagsúla ar CD agus ar láithreán gréasáin ENISA. Déantar plé iomlán ann maidir leis na próisis go léir a thuairiscítear sa doiciméad seo.

Is é an phríomhfhoirmáid a bheidh ann ná Microsoft Project, agus dá bhrí sin is féidir úsáid dhíreach a bhaint as san uirlis bainistíochta tionscadail seo.



Fíor 17 Plean tionscadail



Fíor 18 An plean tionscadail mar aon leis na tascanna go léir agus cuid den chairt Gant

Tá an plean tionscadail ar fáil freisin i bhformaid CVS agus XML. Is féidir tuilleadh faisnéise a fháil ó shaineolaithe ENISA ar chúrsaí CSIRT: cert-relations@enisa.europa.eu!

AGUISÍN

A.1 Tuilleadh ábhair léitheoireachta

Handbook for CSIRTs (CERT/CC)

Saothar tagartha an-chuimsitheach ina bhfuil na topaicí go leir a bhaineann le hobair CSIRT

Foinse: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

Defining Incident Management Processes for CSIRTs: A Work in Progress

Domhain-anailís ar bhainistíocht teagmhas

Foinse: <http://www.cert.org/archive/pdf/04tr015.pdf>

State of the Practice of Computer Security Incident Response Teams (CSIRTs)

Anailís chuimsitheach ar an staid iarbhair i dtaca leis an tírdhreach CSIRT domhanda, lena n-airítear stair, staitisticí agus cuid mhór nithe eile

Foinse: <http://www.cert.org/archive/pdf/03tr001.pdf>

CERT-in-a-box

Cur síos cuimsitheach ar na ceachtanna a foghlaimíodh le linn GOVCERT.NL agus 'De Waarschuwingsdienst' a chur ar bun, is é sin le rá seirbhís náisiúnta Foláireamh na hÍsiltíre.

Foinse: <http://www.govcert.nl/render.html?it=69>

RFC 2350: Expectations for Computer Security Incident Response

Foinse: <http://www.ietf.org/rfc/rfc2350.txt>

NIST³⁷ Computer Security Incident Handling Guide

Foinse: <http://www.securityunit.com/publications/sp800-61.pdf>

ENISA Inventory of CERT activities in Europe

Saothar tagartha ina liostaítear faisnéis faoi CSIRT-anna san Eoraip agus ina liostaítear a gcuid gníomhaíochtaí éagsúla

Foinse: http://www.enisa.europa.eu/cert_inventory/

³⁷ NIST: An Institiúid Náisiúnta Caighdeán agus Teicneolaíochtaí

A.2 Seirbhísí CSIRT

Buíochas ar leith le CERT/CC, a chuir an liosta seo ar fáil

<u>Seirbhísí Freagartha</u>	<u>Seirbhísí Gníomhaíocha</u>	<u>Láimhseáil Déantán</u>
Foláirimh agus Rabhaidh Láimhseáil Teagmhas Anailís Teagmhas Comhordú Freagartha Teagmhas Freagairt Teagmhas ar an láthair Tacaíocht Freagartha Teagmhas Láimhseáil leochaileachta Anailís leochaileachta Freagairt leochaileachta Comhordú freagartha leochaileachta	Fógairtí Faire theicneolaíochta Iniúchtaí nó Measúnachtaí Slándála Cumraíocht agus Cothabháil Slándála Forbairt Uirlisí Slándála Seirbhísí Braite Ionraidh Scaipeadh Faisnéise a Bhaineann le Slándáil	Anailís déantán Freagairt déantán Comhordú freagartha déantán
		<u>Bainistíocht Cháilíochta Slándála</u> Anailís Phriacal Leanúnachas Gnó agus Téarnamh tar éis Tubaiste Sainchomhairle Slándála Méadú Feasachta Oideachas/Oiliúint Measúnú nó Deimhniú Táirgí

Fíor 19 Liosta Seirbhíse CSIRT ó CERT/CC

Cur Síos ar Sheirbhísí

Seirbhísí Freagartha

Tá seirbhísí freagartha ceaptha chun gníomhú i leith iarrataí ar chúnamh, i leith tuairiscí faoi theagmhais ó chliantacht an CSIRT, agus i leith aon bhagairtí nó ionsaithe i gcoinne chórais CSIRT. D'fhéadfadh sé go dtionscnófar roinnt seirbhísí trí fhógra tríú páirtí nó trí fhaireachán féachana nó trí logaí agus trí fholáirimh IDS.

Foláirimh agus Rabhaidh

Baineann an tseirbhís seo le scaipeadh faisnéise ina ndéantar cur síos ar ionsaí ionróra, ar leochaileacht slándála, ar fholáireamh faoi ionradh, ar víreas ríomhaire, nó ar fholáireamh bréige, agus soláthraítear aon bheart gearrthéarmach atá molta chun déileáil leis an bhfadhb. Déantar an foláireamh, an rabhadh nó an t-ábhar comhairleach a sheoladh mar fhreagra ar an bhfadhb reatha lena mbaineann d'fhonn an ghníomhaíocht a chur in iúl don chliant agus d'fhonn treoir a sholáthar maidir lena gcórais a chosaint nó maidir le haon chórais lena mbaineann a aisghabháil. D'fhéadfadh sé go gcruthóidh an CSIRT faisnéis nó d'fhéadfadh sé go n-athdháilfear í tar eis í a fháil ó dhíoltóirí, ó CSIRT-anna eile nó ó shaineolaithe slándála, nó ó chodanna eile den chliantacht.

Láimhseáil Teagmhas

Is é atá i gceist le láimhseáil teagmhas ná iarrataí agus tuairiscí a fháil agus a thriáiseáil, agus gníomhú ina leith, agus anailís a dhéanamh ar theagmhais agus ar imeachtaí.

D'fhéadfadh sé go mbeidh na nithe seo a leanas san áireamh i ngníomhaíochtaí freagartha ar leith:

- beart a ghlacadh chun cosaint a thabhairt do chórais agus gréasáin dá ndéanann gníomhaíocht ionróra difear nó atá faoi bhagairt mar gheall ar ghníomhaíocht den sórt sin
- réitigh agus straitéisí maolaitheacha a sholáthar de réir ábhar comhairleach nó foláireamh ábhartha
- gníomhaíocht ionróra a lorg ar chodanna eile den ghréasán
- trácht gréasáin a scagadh
- córais a atógáil
- córais a phaisteáil nó a dheisiú
- freagraí eile nó straitéisí eatramhacha a fhorbairt

Ó tharla go ndéantar gníomhaíochtaí láimhseála teagmhas a chur i bhfeidhm ar bhealaí éagsúla i gcineálacha éagsúla CSIRT-anna, déantar an tseirbhís a aicmiú tuilleadh de réir na gcineálacha gníomhaíochta a chuirtear i gcrích agus na gcineálacha cúnaimh a thugtar, mar a leanas:

Anailísiú teagmhas

Tá a lán leibhéal anailíse teagmhas ann mar aon lena lán fosheirbhísí. Go bunúsach, is é atá in anailís teagmhas ná scrúdú a dhéanamh ar an bhfaisnéis go léir atá ar fáil agus ar an bhfianaise thacaíochta nó ar dhéantáin a bhaineann le teagmhas nó le himeacht. Is é is cuspóir don anailís ná raon an teagmhais, meid an damáiste a rinneadh de bharr an teagmhais, cineál an teagmhais agus straitéisí freagartha nó réitigh ghearrthéarmacha a shainaithint. D'fhéadfadh sé go n-úsáidfí an CSIRT torthaí na leochaileachta agus na hanailíse ar dhéantáin (mar a thuairiscítear anseo thíos) chun tuiscint a fháil, agus chun an anailís is iomláine agus is nua-aimseartha a sholáthar, maidir leis an teagmhas a tharla ar chóras sonrath. Déanann an CSIRT gníomhaíocht thar theagmhais a chomhghaolú chun aon idirghaolmhaireachtaí, treocheartaí, pátrúin nó síniú ionróra a chinneadh. Seo a leanas dh-fhosheirbhís a d'fhéadfaí a sholáthar mar chuid d'anailís teagmhais, ag brath ar mhisean, aidhmeanna agus próisis an CSIRT:

Bailiú fianaise fóireinsí

Bailiú, caomhnú, taifeadadh agus anailísiú fianaise ó chóras sáraithe ríomhaire chun athruithe ar an gcóras a chinneadh agus chun cabhair a thabhairt maidir le céimeanna éagsúla an tsáraithe. Ní mór bailiú na fianaise a dhéanamh ar shlí ina dtaifeadtar sraith inchruthaithe coimeáda atá inghlactha i gcúirt dlí faoi na rialacha a bhaineann le fianaise. Áirítear an méid seo a leanas sna tascanna a ghabhann le bailiú fianaise fóireinsí (ach níl sé teoranta do na nithe sin amháin): cóip íomhá giotán a dhéanamh de thiomantán crua an chórais lena mbaineann; seiceáil a dhéanamh i dtaobh ar tharla aon athruithe ar an gcóras, mar shampla ríomhchláir nua, comhaid nua, seirbhísí nua agus úsáideoirí nua; féachaint ar phróisis reatha agus poirt oscailte; agus seiceáil a dhéanamh maidir le ríomhchláir agus sraitheanna uirlisí Traíoch. D'fhéadfadh sé go mbeidh ar na baill foirne CSIRT a chomhlíonann an fheidhm seo sásta gníomhú mar fhinné saineolach in imeachtaí cúirte.

Rianú nó lorgaireacht

Rianú tionscnaimh ionróra nó na córais a raibh rochtain ag an ionróir orthu a

shainaithint. D'fhéadfadh sé gurb é atá i gceist leis an ngníomhaíocht seo ná rianú nó lorgaireacht a dhéanamh maidir leis an tslí ina ndeachaigh an t-ionróir isteach sna córais agus sna gréasáin ghaolmhara lena mbaineann, maidir leis na córais a úsáideadh chun rochtain a fháil, maidir leis an áit inar tionscnaíodh an t-ionsaí, agus maidir leis na córais agus na gréasáin eile a úsáideadh mar chuid den ionsaí. D'fhéadfadh sé freisin go mbeidh gá le hiarracht a dhéanamh céannacht an ionróra a chinneadh. D'fhéadfadh sé gur aon duine amháin a dhéanfaidh an obair seo ach, de ghnáth, déantar í i gcomhar le pearsanra forfheidhmithe dlí, le solathróirí seirbhísí idirlín nó le heagraíochtaí eile atá bainteach leis an ábhar.

Freagairt teagmhas ar an láthair

Soláthraíonn an CSIRT cúnamh díreach ar an láthair chun cabhrú le cliaint téarnamh a dhéanamh tar eis teagmhais. Déanann an CSIRT féin anailís fhisiciúil ar na córais lena mbaineann agus cuireann sé deisiú agus aisghabháil na gcóras a chur i ngníomh, in ionad gan ach tacaíocht freagartha a sholáthar le teileafón nó le ríomhphost (féach anseo thíos). Is é atá i gceist leis an tseirbhís seo ná na gníomhartha go léir a dhéantar ag an leibhéal áitiúil ar gníomhartha iad atá riachtanach má tá amhras ann gur tharla teagmhas nó más rud é go dtarlaíonn teagmhas. Mura bhfuil an CSIRT suite sa suíomh sáraithe, rachadh na baill foirne chuig an suíomh agus chuirfidís an obair i gcrích ansin. I gcásanna eile, d'fhéadfadh sé go mbeidh foireann áitiúil ar an láthair agus freagairt teagmhas á soláthar aici mar chuid dá hobair laethúil. Is fíor sin go háirithe má sholáthraítear láimhseáil teagmhas mar chuid de ghnáthfheidhm an chórais, an ghréasáin nó na riarthóirí slándála in ionad CSIRT arna bhunú go sonrach.

Tacaíocht freagartha teagmhas

Tugann an CSIRT cabhair agus treoir d'íospartach (d'íospartaigh) an ionsaí le linn téarnamh a dhéanamh tar eis teagmhais agus déantar sin le teileafón, le ríomhphost, le facs nó i bhfoirm doiciméid. D'fhéadfadh sé gurb é a bheadh i gceist leis sin ná cúnamh teicniúil maidir le léiriú na sonraí a bailíodh, faisnéis teagmhála a sholáthar nó treoir a chur ar fáil faoi threoir maidir le straitéisí maolaithe agus téarnaimh. Níl aon ghníomhartha freagartha teagmhais díreacha, ar an láthair ann den chineál a thuairiscítear thuas. Ina ionad sin, soláthraíonn an CSIRT treoir ar mhodh cianda agus, dá bhrí sin, is féidir leis an bhfoireann féin na bearta téarnaimh a dhéanamh iad féin.

Comhordú freagartha teagmhas

Comhordaíonn an CSIRT an iarracht freagartha i measc na bpáirtithe atá bainteach leis an teagmhas. De ghnáth, is iad atá san áireamh ná íospartach an ionsaí, láithreáin eile atá bainteach leis an ionsaí agus aon láithreáin nach mór cúnamh a thabhairt dóibh le linn an t-ionsaí a anailísiú. D'fhéadfadh sé freisin go mbeadh páirtithe i gceist a sholáthraíonn tacaíocht IT don íospartach, mar shampla solathróirí seirbhísí idirlín, CSIRT-anna eile agus riarthóirí córais agus gréasáin ar an láthair lena mbaineann. D'fhéadfadh sé gur ghá, mar chuid den obair comhordaithe, faisnéis teagmhála a bhailiú, eolas a thabhairt do láithreáin áirithe maidir le baint ionchasach leis an ábhar (mar íospartach nó mar fhoinsé ionsaí), staitisticí a bhailiú faoin líon láithreán atá i gceist, agus malartú agus anailísiú faisnéise a éascú. D'fhéadfadh sé gur ghá, mar chuid den obair comhordaithe, fógraí a thabhairt do chomhairleoir dlí nó do ranna acmhainn i daonna nó caidreamh poiblí eagraíochta áirithe, agus comhoibriú leo. Bheadh comhordú le lucht forfheidhmithe an dlí i gceist freisin. Ní bhaineann an tseirbhís seo le freagairt dhíreach ar an láthair.

Láimhseáil leochaileachta

Is é atá i gceist le láimhseáil leochaileachta ná faisnéis agus tuairiscí a ghlacadh maidir le leochaileachtaí crua-earraí agus bogearraí; anailís a dhéanamh ar chineál, ar mheicníochtaí agus ar éifeachtaí na leochaileachtaí; agus straitéisí freagartha a fhorbairt chun leochaileachtaí a bhraith agus a dheisiú. Ó tharla go ndéantar láimhseáil leochaileachtaí a chur i bhfeidhm ar shlí éagsúla ag cineálacha éagsúla CSIRT-anna, déantar an tseirbhís seo a aicmiú tuilleadh de réir na gcineálacha gníomhaíochtaí a dhéantar agus de réir na gcineálacha cúnamh a thugtar, mar a leanas:

Anailís leochaileachta

Déanann an CSIRT anailís theicniúil agus scrúdú teicniúil ar leochaileachtaí i gcrua-earraí nó i mbogearraí. Áirítear san obair sin fíorú leochaileachtaí a cheaptar atá ann agus scrúdú teicniúil na leochaileachta crua-earraí nó bogearraí lena chinneadh cén áit a bhfuil sí agus conas is féidir í a dhúshaothrú. D'fhéadfadh sé go n-aireofar san anailís athbhreithniú a dhéanamh ar an bhfoinse-chód trí leas a bhaint as dífhachtóir chun a chinneadh cén áit a dtarlaíonn an leochaileacht nó trí iarracht a dhéanamh an fhadhb a athchruthú ar chóras tástála.

Freagairt leochaileachta

Baineann an tseirbhís seo leis an bhfreagairt chuí a chinneadh d'fhonn leochaileacht a mhaolú nó a dheisiú. D'fhéadfadh sé gurb é a bheadh i gceist ná paistí, réitigh iomlána agus réitigh shealadacha a fhorbairt. Baineann sé freisin le scéala a thabhairt do pháirtithe eile maidir leis an straitéis maolaithe, trí ábhar comhairleach nó foláirimh a chruthú agus a dháileadh, b'fhéidir. D'fhéadfadh sé go gcuirfí an fhreagairt maidir leis an tseirbhís seo i bhfeidhm trí phaistí, réitigh iomlána nó réitigh shealadacha a shuiteáil.

Comhordú freagartha leochaileachta

Cuireann an CSIRT an leochaileacht in iúl do na codanna éagsúla den chliantacht agus roinneann sé faisnéis faoi conas dul i mbun an leochaileachta a réiteach nó a mhaolú. Fíoraíonn an CSIRT go ndearnadh an straitéis freagartha leochaileachta a chur i bhfeidhm go rathúil. D'fhéadfadh sé go n-aireofar sa tseirbhís seo cumarsáid a dhéanamh le díoltóirí, le CSIRT-anna eile, le saineolaithe teicniúla, le baill den chliantacht agus leis na daoine aonair nó na grúpaí a tháinig ar an leochaileacht i dtosach báire nó a thuairiscigh í. Áirítear i ngníomhaíochtaí éascaíocht a dhéanamh maidir leis an anailís ar leochaileacht nó maidir leis an tuairisc faoi leochaileacht, comhordú a dhéanamh ar an sceideal ar dá réir a scaoilfear doiciméid chomhfhreagracha, paistí nó réitigh shealadacha; agus sintéisiú a dhéanamh ar an anailís theicniúil arna déanamh ag páirtithe éagsúla. D'fhéadfadh sé freisin go mbeidh san áireamh sa tseirbhís seo cartlann phoiblí nó cartlann phríobháideach nó bunachair eolais a choimeád maidir le faisnéis leochaileachta agus straitéisí comhfhreagracha freagartha.

Láimhseáil Déantán

Is é atá i ndéantán ná aon chomhad nó rud a fhaightear ar chóras agus a bhféadfadh baint a bheith aige le tóraíocht nó ionsaí i gcórais nó i ngréasain nó atá á úsáid chun bearta slándála a shárú. D'fhéadfadh na nithe seo a leanas a bheith san áireamh i ndéantáin, gan iad a bheith teoranta dóibh: víris ríomhaire, ríomhchláir Thraíoch, worm-anna, scrípteanna dúshaothraithe agus sraitheanna uirlisí.

Baineann laimhseail déantán le faisnéis a ghlacadh maidir le cóipeanna de dhéantáin a úsáidtear in ionsaithe ó ionróirí, i dtaiscéalaíocht agus i ngníomhaíochtaí neamhúdaraíthe nó suaiteacha eile. Nuair a fhaightear é, déantar an déantán a athbhreithniú. Áirítear san athbhreithniú anailís a dhéanamh ar chineál, ar mheicníochtaí, ar leagan agus ar úsáid na ndéantán; agus forbairt a dhéanamh ar straitéisí freagartha (nó straitéisí freagartha a mholadh) chun na déantáin sin a bhraith agus a dhíothú agus chun cosaint a dhéanamh ina gcoinne. Ó tharla go ndéanann CSIRT-anna gníomhaíochtaí láimhseála déantán a chur i bhfeidhm ar shlite éagsúla, déantar an tseirbhís seo a aicmiú tuilleadh de réir na gcineálacha gníomhaíochtaí a dhéantar agus na gcineálacha cúnaimh a thugtar, mar a leanas:

Anailís déantán

Comhlíonann an CSIRT scrúdú teicniúil agus anailís theicniúil ar aon déantán a fhaightear ar chóras. D'fhéadfadh sé gurb é atá i gceist leis an anailís a dhéantar ná an cineál comhaid agus struchtúr an déantáin a shainaithint, déantán nua a chur i gcomparáid le déantáin láithreacha nó le leaganacha eile den déantán céanna chun cosúlachtaí agus difríochtaí a fheiceáil, nó ais-innealtóireacht nó díchóimeáil cóid a dhéanamh chun a chinneadh cén cuspoir agus cén fheidhm atá ag an déantán.

Freagairt déantán

Baineann an tseirbhís seo leis na gníomhartha cuí a chinneadh chun déantáin a bhraith agus a aistriú amach as córas, chomh maith le gníomhartha chun cosc a chur ar dhéantáin a shuiteáil. D'fhéadfadh sé gurb é a bheadh i gceist leis sin ná sínithe a chruthú ar feidir iad a chur le bogearraí frithviris nó IDS.

Comhordú freagartha déantán

Baineann an tseirbhís seo le torthaí agus straitéisí freagartha a bhaineann le déantán a chomhroinnt agus ashintéisiú le taighdeoirí, le CSIRT-anna, le díoltóirí agus le saineolaithe slándála eile. Áirítear sna gníomhaíochtaí scéala a chur chuig páirtithe eile agus anailís theicniúil ó fhoinsí éagsúla a shintéisiú. D'fhéadfadh sé go mbeidh san áireamh i ngníomhaíochtaí eile cartlann phoiblí nó cartlann chliant a choimeád maidir le déantáin atá ar eolas agus ar a dtionchar agus maidir le straitéisí comhfhreagracha freagartha.

Seirbhísí Gníomhaíocha

Tá seirbhísí gníomhaíocha ceaptha chun feabhas a chur ar bhonneagar agus ar phróisis slándála na cliantachta sula dtarlaíonn aon teagmhas nó imeacht nó sula ndéantar aon teagmhas nó imeacht a bhraith. Is iad na príomhaidhmeanna ná teagmhais a sheachaint agus a dtionchar agus a raon a laghdú nuair a tharlaíonn siad.

Fógairtí

Tá na nithe seo a leanas san áireamh sa reimse seo, gan a bheith teoranta dóibh: foláirimh maidir le hionradh, rabhaidh leochaileachta, agus ábhar comhairleach maidir le slándáil. Trí fhógairtí den sórt sin, cuirtear forbairtí nua in iúl do chliant ar forbairtí iad lena ngabhann tionchar meántéarmach go dtionchar fadtéarmach, mar shampla leochaileachtaí a bhfuiltear tar éis teacht orthu nó uirlisí ionróra. Cumasaíonn fógairtí do chliant a gcórais agus a ngréasáin a chosaint ar fhadhbanna a bhfuiltear tar éis teacht orthu agus sin a dhéanamh sular féidir le haon duine iad a dhúshaothrú.

Faire theicneolaíochta

Déanann an CSIRT faireachán agus breathnóireacht ar fhorbairtí nua teicniúla, ar ghníomhaíochtaí ionróirí agus ar threochtaí gaolmhara d'fhonn cabhair a thabhairt maidir le bagairtí todhchaí a shainaithint. Is féidir na topaicí a athbhreithnítear a leathnú ionas go gcuirtear san áireamh rialuithe dlíthiúla agus reachtacha, bagairtí sóisialta nó polaitíochta, agus teicneolaíochtaí atá ag teacht chun cinn. Baineann an tseirbhís seo le liostaí seoltaí poist, láithreáin ghréasáin slándála agus ailt reatha nuachta agus irisleabhair i réimsí na heolaíochta, na teicneolaíochta, na polaitíochta agus rialtais a léamh d'fhonn faisnéis a fháil atá ábhartha do chórais agus go ghréasáin na gcliantachtaí. D'fhéadfadh sé go mbeidh san áireamh sa réimse seo cumarsáid a dhéanamh le páirtithe eile atá ina n-údaráis sna réimsí seo d'fhonn a chinntiú go bhfaighfear an fhaisnéis nó an léiriú is fearr agus is cruinne. D'fhéadfadh sé gurb é a thiocfadh as an tseirbhís seo ná fógairt, treoirlinnte nó moltaí de chineál éigin atá dírithe ar shaincheistanna slándála níos meánréimhsí/fadtréimhsí.

Iniúchtaí nó Measúnachtaí Slándála

tríd an tseirbhís seo, soláthraítear athbhreithniú agus anailísiú mionsonraithe ar bhonneagar slándála eagraíochta, agus é bunaithe ar na riachtanais arna sainmhíniú ag an eagraíocht nó le caighdeáin eile tionscail a bhhfuil feidhm acu. D'fhéadfadh sé freisin go mbeadh athbhreithniú ar chleachtais slándála eagraíochta i gceist. Tá a lán cineálacha iniúchtaí nó measúnachtaí ar fáil, lena n-áirítear:

Athbhreithniú ar an mBonneagar

Athbhreithniú láimhe a dhéanamh ar chumraíochtaí crua-earraí agus bogearraí, ar ródairí, ar bhallaí dóiteáin, ar fhreastalaithe agus ar fheistí deisce chun a chinntiú go bhfuil siad in oiriúint do dhea-chleachtas eagraíochta nó tionscail i dtaca le polasaithe slándála agus cumraíochtaí caighdeánacha de.

Athbhreithniú ar dhea-chleachtas

Agallamh a dhéanamh le fostaithe agus le riarthóirí córais agus gréasáin lena chinneadh an bhfuil a gcleachtais slándála in oiriúint do don pholasaí sainmhínte slándála eagraíochta nó do chaighdeáin áirithe tionscail.

Scanadh

Scanóirí leochaileachta nó víris a úsáid chun a chinneadh cé na córais agus na gréasáin atá leochaileach.

Tástáil treáite

Slándail laithreáin a thástáil trí ionsaí d'aon turas a dhéanamh ar a chórais agus ar a ghréasáin.

Ní mór ceadú a fháil ó bhainisteoirí sinsearacha roimh iniúchtaí nó measúnachtaí den sórt seo a dhéanamh. D'fhéadfadh sé go mbeadh cosc ar ghníomhaíochtaí den sórt sin mar gheall ar pholasaí eagraíochta. D'fhéadfadh sé go mbeadh i gceist le soláthar na seirbhíse seo forbairt a dhéanamh ar shraith choiteann cleachtas ar ina n-aghaidh a dhéantar na tástálacha nó na measúnachtaí, mar aon le forbairt a dhéanamh ar shraith scileanna riachtanacha don fhoireann a chuireann an tástáil, na measúnachtaí, na hiniúchtaí nó na hathbhreithnithe i gcrích. D'fhéadfaí an tseirbhís seo a asfhoinsiú freisin chuig conraitheoir tríú páirtí nó chuig soláthróir seirbhíse bainistithe slándála ag a bhfuil

an oilteacht chuí maidir le hiniúchtaí agus measúnachtaí a sheoladh.

Cumraíocht agus Cothabháil Uirlisí, Feidhmiúchán, Bonneagar agus Seirbhísí Slándála

Leis an tseirbhís seo, sainaitnítear nó soláthraítear treoir chuí i dtaobh conas déileáil le cumraíocht agus cothabháil dhaingean uirlisí, feidhmiúchán agus bonneagair ghinearálta a úsaideann cliantacht an CSIRT nó an CSIRT é féin. Ar leith ó threoir a sholáthar, féadfaidh an CSIRT uasdátú cumraíochta agus cothabháil a dhéanamh maidir le huirlisí agus seirbhísí slándála, mar shampla IDS, scanadh gréasán nó córas faireachán, scagairí, rapair, ballaí dóiteáin, gréasáin phríobháideacha fhíorúla (VPN), nó meicníochtaí fíordheimhniúcháin. D'fhéadfadh sé freisin go soláthródh an CSIRT na seirbhísí sin mar chuid dá bpríomhfheidhm. D'fhéadfadh sé freisin go ndéanfaidh an CSIRT cumraíocht agus cothabháil i ndáil le freastalaithe, deasca, ríomhaire glúine, cúntóirí pearsanta digiteacha (PDA-anna), agus feistí eile gan sreang ach sin de réir treoirlinnte slándála. Áirítear sa tseirbhís aon saincheisteanna nó fadhbanna a bhaineann le cumraíochtaí nó le húsáid uirlisí agus feidhmiúcháin agus a measann an CSIRT ina leith go bhféadfadh sé go bhfuil an córas inionsaithe a chur faoi bhráid an lucht bainistíochta.

Forbairt Uirlisí Slándála

Áirítear sa tseirbhís seo forbairt a dhéanamh ar aon uirlisí nua a bhaineann go sonrach le cliant agus atá de dhíth ar an gcliantacht nó ag an CSIRT nó ag teastáil uathu. Mar shampla, d'fhéadfadh se go mbeadh san áireamh sa réimse seo paistí slándála a fhorbairt le haghaidh sain-bhogearraí a úsaideann an chliantacht nó dáileadh bogearraí daingnithe atá inúsáidte chun óstaigh sháraithe a atógáil. D'fhéadfadh sé go mbeadh san áireamh ann freisin forbairt a dhéanamh ar uirlisí nó ar scripteanna lena leathnaítear feidhmiúlacht uirlisí láithreacha slándála, mar shampla breiseán nua do scanóir leochaileachta nó gréasáin, scripteanna trína n-éascaítear úsáid teicneolaíochta criptithe nó meicníochtaí dáiliúcháin uathoibrithe le haghaidh paistí.

Seirbhísí Braite Ionraidh

I gcás CSIRT-anna a sholáthraíonn an tseirbhís seo, déanann siad athbhreithniú ar logaí láithreacha IDS, anailísíonn agus tionscnaíonn siad freagra maidir le haon teagmhais a thagann faoi reim a dtairsí sainmhínithe nó cuireann siad ar aghaidh aon fholáirimh de réir comhaontaithe réamhshainmhínithe leibhéil seirbhíse nó de réir straitéise maidir le nithe a chur faoi bhráid na hardbhainistíochta. D'fhéadfadh sé gur tasc deacair é ionradh a bhraith agus anailísiú a dhéanamh ar na logaí gaolmhara slándála—ní amháin le linn a chinneadh cén áit ina suífead na braiteoirí laistigh den timpeallacht ach freisin le linn na méideanna móra sonraí a bhailiú agus a anailísiú ina dhiaidh sin. Ina lán cásanna, tá gá le sainuirlisí nó sainoilteacht chun sintéisiú agus léiriú a dhéanamh ar an bhfaisnéis d'fhonn aláraim bhréige, ionsaithe nó imeachtaí gréasáin a shainaitheint agus d'fhonn straitéisí a chur i bhfeidhm chun deireadh a chur le himeachtaí den sórt sin nó chun iad a íoslaghdú. Roghnaíonn roinnt eagraíochtaí an ghníomhaíocht seo a asfhoinsiú chuig páirtithe eile ag a bhfuil níos mó oilteachta maidir leis na seirbhísí seo a chur i gcrích, mar shampla soláthróirí seirbhíse bainistithe slándála.

Scaipeadh Faisnéise a Bhaineann le Slándáil

Tríd an tseirbhís seo, solathraítear bailiúchán cuimsitheach sorochtana faisnéise úsáidí do chliant ar bailiúchán é a thugann cabhair i dtaca le slándáil a fheabhsú. D'fhéadfadh sé go mbeadh na nithe seo a leanas san áireamh san fhaisnéis sin:

- treoirlínte tuairiscithe agus faisnéis teagmhála don CSIRT
- cartlanna foláireamh, rabhadh agus fógartí eile
- doiciméid faoi dhea-chleachtas reatha
- treoir ghinearálta maidir le ríomhairí
- polasaithe, nósanna imeachta agus seicliostaí
- forbairt paistí agus faisnéis dailiúcháil
- nascanna díoltóirí
- staitisticí agus treochtaí reatha maidir le tuairisciú teagmhas
- faisnéis eile a d'fhéadfadh feabhas a chur ar chleachtais slándála i gcoitinne

Is féidir leis an CSIRT nó ag cuid eile den eagraíocht (IT, acmhainní daonna nó caidreamh na meán) an fhaisnéis seo a fhorbairt agus a fhoilsiú agus is féidir faisnéis a bheith san áireamh inti ó acmhainní seachtracha ar nós CSIRT-anna eile, díoltóirí agus saineolaithe slándála.

Seirbhísí Bainistíochta Cháilíochta Slándála

Níl na seirbhísí a thagan faoi reim na catagóra seo bainteach le laimhseáil teagmhas ná le CSIRT-anna amháin. Is seirbhísí iad a bhfuil eolas maith ann ina leith agus atá seanbhunaithe agus tá siad ceaptha chun feabhas a chur ar shlándáil fhoriomlán eagraíochta. trí leas a bhaint as an taithí atá faighte ó na seirbhísí freagarthacha agus gníomhaíochta a thuairiscítear thuas, is féidir le CSIRT peirspictíochtaí uathúla a chur ar fáil maidir leis na seirbhísí bainistíochta ardchaighdeán seo ar peirspictíochtaí iad nach mbeadh ar fail thairis sin b'fhéidir. Tá na seirbhísí seo ceaptha chun aiseolas agus ceachtanna a foghlaimíodh a ionchorprú, ar aiseolas agus ceachtanna iad atá bunaithe ar eolas a fuarthas trí ghníomhú i leith teagmhas, leochaileachtaí agus ionsaithe. Trí thaithí den sórt sin a chur san áireamh sna seirbhísí seanbhunaithe traidisiúnta (arna dtuairisciú thíos) mar chuid de phróiseas bainistíochta ardchaighdeán slándála, is féidir feabhas a chur ar iarrachtaí fadtéarmacha slándála in eagraíocht. Ag brath ar struchtúir agus freagrachtaí eagrúcháin, féadfaidh CSIRT na seirbhísí sin a sholáthar nó pairt a ghlacadh iontu mar chuid d'iarracht foirne níos mó de chuid eagraíochta.

Leis na tuairiscí seo a leanas, mínítear conas is féidir le hoilteacht CSIRT dul chun tairbhe gach ceann de na seirbhísí bainistíochta ardchaighdeán slándála seo.

Anailís Phriacail

D'fhéadfadh sé go mbeadh CSIRT-anna in ann breisluach a chur le hanailísiú agus measúnú priacal. Is féidir leis sin feabhas a chur ar chumas na heagraíochta fíorbhagairtí a mheas, measúnachtaí réadúla, idir chainníochtúil agus cháilíochtúil, a dhéanamh ar na priacail atá ann do shócmhainní faisnéise agus measúnú a dhéanamh ar straitéisí cosanta agus freagartha. I gcás CSIRT-anna a sholáthraíonn an tseirbhís seo, sheolfaidís gníomhaíochtaí anailíse priacal faisnéise slándála i dtaca le córais nua agus próisis nua gnó de, nó thabharfaidís cabhair ina leith sin, nó dhéanfaidís measúnú ar bhagairtí agus ionsaithe i gcoinne sócmhainní agus córas cliant.

Leanúnachas Gnó agus Pleanáil maidir le Téarnamh tar eis Tubaiste

Mar gheall ar nithe a tharla san am a caitheadh agus ar thuartha faoi threochtaí maidir le

teagmhais agus slándáil, tá sé de chumas ag líon méadaitheach teagmhas díghrádú tromchúiseach a dhéanamh ar oibríochtaí gnó. Dá bhrí sin, le linn iarrachtaí pleanála is ceart breithniú a dhéanamh ar thaithí agus ar mholtaí CSIRT-anna le linn a chinneadh conas gníomhú má tharlaíonn teagmhais den sórt sin d'fhonn leanúnachas oibríochtaí gnó a chinntiú. I gcás CSIRT-anna atá ag gabháil don tseirbhís seo, déanann siad pleanáil maidir le leanúnachas gnó agus téarnamh tar éis tubaiste ar eagla go dtarlódh imeachtaí a bhaineann le bagairtí agus ionsaithe ar ríomhairí.

Sainchomhairle Slándála

Is féidir CSIRT-anna a úsáid chun comhairle agus treoir a sholáthar maidir le dea-chleachtas slándála is ceart a chur i bhfeidhm i gcomhair oibríochtaí gnó cliant. I gcás CSIRT a sholáthraíonn an tseirbhís seo, bíonn sé bainteach le moltaí a ullmhú nó riachtanais a shainaithint maidir le ceannach, suiteáil nó daingniú córas nua, feistí gréasáin, feidhmiúchán bogearraí nó próiseas gnó uile-fhiontair. Áirítear sa tseirbhís seo treoir agus cúnamh a sholáthar le linn forbairt a dhéanamh ar polasaithe slándála eagraíochta nó cliantachta. D'fhéadfadh sé a bheith bainteach le fianaise nó comhairle a sholáthar do chomhlachtaí reachtacha nó do chomhlachtaí rialtais eile.

Méadú Feasachta

D'fhéadfadh sé go mbeadh CSIRT-anna in ann a thaispeáint cé na réimsí ina bhfuil tuilleadh faisnéise agus teorach a teastail ó chliaint ionas gur fearr a bheidh cleachtais slándála inghlactha agus polasaithe slándála eagraíochta á gcomhlíonadh acu. Trí mhéadú a dhéanamh ar fheasacht ghinearálta na gcliant ar shlándáil, ní amhain go gcuirtear feabhas ar a dtuiscint ar shaincheisteanna slándála ach freisin is cuidiú é maidir le comhlíonadh a ndualgas laethúil ar shlí níos daingne. D'fhéadfadh sé sin laghdú a dhéanamh ar líon na n-ionsaithe rathúla agus méadú a dhéanamh ar an dóchúlacht go ndéanfaidh cliaint ionsaithe a bhraith agus a thuairisciú agus, sa dóigh sin, déanfar laghdú ar amanna téarnaimh agus cuirfear deireadh le cailleanais nó íoslaghdófar iad.

I gcás CSIRT-anna a sholáthraíonn an tseirbhís seo, lorgaíonn siad deiseanna chun feasacht slándála a mhéadú trí fhorbairt a dhéanamh ar ailt, ar phóstaí, ar nuachtlitreacha, ar láithreáin ghréasáin nó ar acmhainní faisnéise eile trína mínítear dea-chleachtas agus trína soláthraítear comhairle maidir le réamhchúraimí atá le glacadh. D'fhéadfadh sé freisin go n-áireofar sna gníomhaíochtaí cliaint a choimeád cothrom le dáta maidir le nósanna imeachta leanúnacha slándála agus maidir le bagairtí ionchasacha ar chórais eagraíochta.

Oideachas/Oiliúint

Baineann an tseirbhís seo le faisnéis a sholáthar do chliaint maidir le saincheisteanna slándála ríomhaire trí leas a bhaint as seimineáir, ceardlanna, cúrsaí agus ranganna teagaisc. D'fhéadfadh an méid seo a leanas a bheith i gceist: treoirlínte maidir le tuairisciú teagmhas, modhanna cuí freagartha, uirlisí freagartha teagmhas, modhanna coiscthe teagmhas agus faisnéis eile atá riachtanach chun cosaint, braith, tuairisciú agus gníomhú a dhéanamh maidir le teagmhais slándála ríomhaire.

Measúnú nó Deimhniú Táirgí

I gcomhair na seirbhíse seo, d'fhéadfadh sé go seolfadh an CSIRT measúnachtaí ar uirlisí, ar fheidhmiúcháin nó ar sheirbhísí eile chun slándáil na dtáirgí a chinntiú agus



chun a chinntiú go gcomhlíonann siad cleachtais inghlactha slándála CSIRT nó eagraíochta. Is féidir uirlisí agus feidhmiúcháin a athbhreithnítear a bheith san earnáil foinse oscailte nó is féidir táirgí tráchtála a bheith i gceist. Is féidir an tseirbhís seo a sholáthar mar mheasúnú nó trí ríomhchlár deimhniúcháin, ag brath ar na caighdeáin a chuirtear i bhfeidhm san eagraíocht nó sa CSIRT.

A.3 Na samplaí

CSIRT samhailteach

Beart 0 - Tuiscint a fháil ar céard é CSIRT:

Ní mór don CSIRT samplach fónamh d'institiúid mheánmhéide ina bhfuil 200 fostaí. Tá a roinn IT féin ag an institiúid mar aon le dhá oifig chraoibhe sa tír chéanna. Tá ról tábhachtach ag IT sa chuideachta mar go n-úsáidtear é le haghaidh cumarsáide inmheánaí, le haghaidh gréasáin sonraí agus le haghaidh ríomhghnó 24x7. Tá a gréasán féin ag an institiúid agus diúscaíonn sí ceangal iomarcach leis an idirlíon trí dhá ISP éagsúla..

Beart 1: An chéim thosaigh

Ag an gcéim thosaigh, déantar an CSIRT nua a phleanáil mar CSIRT Inmheánach agus soláthraítear a chuid seirbhísí don chuideachta óstach, don roinn IT áitiúil agus don fhoireann. Déanann sé tacaíocht agus comhordú a sholáthar freisin in oifigí craoibhe éagsúla maidir le láimhseáil teagmhas a bhaineann le slándáil.

Beart 2: Na seirbhísí cearta a roghnú

Ag an gcéim thosaigh, cinntear go ndíreofar an CSIRT nua go príomha ar roinnt seirbhísí lárnacha a sholáthar do na fostaíthe.

Cinntear go ndéanfar breithniú, tar éis céime píolóta, i dtaobh leathnú an bhirt seirbhísí agus i dtaobh tús a chur le roinnt 'Seirbhísí Bainistíochta Slandála'. Déanfar an cinneadh sin de réir an aiseolais a fhaightear ó na cliaint phíolóta agus i ndlúthchomhar leis an roinn Deimhnithe Cáilíochta.

Beart 3: Anailís a dhéanamh ar an gcliantacht agus ar na bealaí cuí cumarsáide

Mar thoradh ar sheisiún dianmhachnaimh le roinn daoine ardleibhéil sa lucht bainistíochta agus sa chliantacht, gineadh dóthain ionchuir le haghaidh anailís SWOT. Is é a lean as sin ná an tuairim go raibh gá leis na seirbhísí lárnacha seo a leanas:

- Foláirimh agus rabhaidh
- Láimhseáil teagmhas (anailís, tacaíocht fhreagartha agus comhordú freagartha)
- Fógairtí

Ní mór a chinntiú go ndéantar an fhaisnéis a dháileadh ar shlí dhea-eagraithe ionas go sroichte an chuid is mó den chliantacht is féidir. Dá bhrí sin, cinntar go ndéanfar foláirimh, rabhaidh agus fógairtí i bhfoirm ábhair chomhairligh slándála a fhoilsiú ar shainláithreán gréasáin agus a dháileadh trí leas a bhaint as liosta seoltaí ríomhphoist. Is féidir CSIRT a úsáid chun tuairiscí teagmhais a fháil trí ríomhphoist, le teileafón agus le facs. Tá sé beartaithe go mbeidh foirm ghréasáin aontaithe ann mar chéad bheart eile.

Beart 4: Ráiteas Misin

Tá an raiteas misin seo a leanas déanta ag lucht bainistíochta an CSIRT shamhailtigh:

“Soláthraíonn CSIRT Samhailteach faisnéis agus cúnamh d’fhoireann a chuideachta óstaí chun laghdú a dhéanamh ar na priacail go mbeidh teagmhais slándála ríomhaire ann chomh maith le gníomhú má tharlaíonn teagmhais den sórt sin.”

Sa tslí sin, cuireann an CSIRT samhailteach seo in iúl go soiléir gur CSIRT inmheanach é agus gurb é atá ina ghnó lárnach ná déileáil le saincheistanna a bhaineann le slándáil IT.

Beart 5: An Plean Gnó a Phleanáil**An múnla airgeadais**

Ó tharla go bhfuil ríomhgnó 24x7 ag an gcuideachta, mar aon le roinn IT 24x7, déantar cinneadh seirbhís iomlán a sholáthar le linn uaire oifige agus seirbhís ar ghlaoch a sholáthar lasmuigh d’uaire oifige. Déanfar na seirbhísí don chliantacht a sholáthar saor in aisce, ach déanfar an cumas maidir le seirbhísí a sholáthar do chustaiméirí seachtracha a mheasúnú le linn na céime píolóta agus na céime measúnachta.

An múnla ioncaim

Le linn na céime tosaigh agus na céime píolóta, déanfar an CSIRT a mhaoiniú tríd an gcuideachta óstach. Le linn na céime píolóta agus na céime measúnaithe déanfar maoiniú breise a phlé agus cuirfear san áireamh an seans go bhféadfaí seirbhísí a bheith á ndíol le custaiméirí seachtracha.

An múnla eagrúcháin

Is cuideachta bheag í an eagraíocht óstach agus, dá bhrí sin, roghnaítear an múnla leabaithe.

Le linn uaire oifige, soláthróidh foireann triúr duine na seirbhísí lárnacha (ábhar comhairleach slándála a scaipeadh agus láimhseáil/comhordú teagmhas).

Tá daoine ag a bhfuil scileanna oiriúnacha ar fostú cheana féin ag roinn IT na heagraíochta. Déantar comhaontú leis an roinn sin ionas gur féidir an CSIRT nua tacaíocht a iarraidh ar bhonn ad-hoc nuair is gá sin. Chomh maith leis sin, is féidir leas a bhaint as an 2^ú líne dá dteicneoirí ar glaoch.

Beidh foireann lárnach CSIRT ann ina mbeidh ceathrar ball lánaimseartha agus cúigear ball breise CSIRT. Tá duine amháin díobh sin ar fáil freisin ar sheal athfhillteach.

Foireann

Tá cúlra ag ceannaire na foirne CSIRT i gcúrsaí slándála agus i dtacaíocht 1^ú agus 2^ú leibhéal agus tá taithí aige ar obair sa réimse bainistíochta athléimneachta i gcás géarchéimeanna. Is speisialtóirí slándála iad an triúr ball foirne eile. Tá baill foirne CSIRT páirtaimseartha na roinne IT ina speisialtóirí sa chuid de bhonneagar na cuideachta a bhaineann leo.

Beart 5 – Úsáid na hoifige agus an polasaí slándála faisnéise Trealamh agus suíomh na hoifige

Ó tharla go bhfuil slándáil fhisiciúil éifeachtúil i bhfeidhm ag an gcuideachta óstach, tá an CSIRT nua clúdaithe go maith i dtaca leis sin de. Soláthraítear seomra ar a dtugtar “seomra cogaidh” le gur féidir comhordú a dhéanamh i gcás éigeandála. Ceannaítear taisceadán le haghaidh an ábhair criptiúcháin agus le haghaidh doiciméad fogair. Bunaíodh líne theileafóin ar leithligh, lena n-áirítear lasc-chlár mar éascaíocht i gcomhair líne éigeandála le linn uaire oifige, agus fón póca dualgais shoghluaiste “ar glaoch” le haghaidh amanna lasmuigh d’uaire oifige, agus an uimhir chéanna aige leis an líne éigeandála.

Is féidir trealamh láithreach agus an láithreán gréasáin corparáideach le haghaidh fógairtí a bhaineann le CSIRT a úsáid freisin. Déantar liosta seoltaí poist a shuiteáil agus a chothabháil agus tá cuid shrianta ann le haghaidh cumarsáidí idir ceannairí foirne agus le foirne eile. Déantar na mionsonraí go léir faoi bhaill foirne a stóráil i mbunachar sonraí agus coimeádtar leagan clóite sa taisceadán.

Rialáil

Ó tharla go bhfuil an CSIRT leabaithe i gcuideachta ag a bhfuil polasaithe slándála cheana féin, bunaíodh na polasaithe rochtana don CSIRT a bhunú le cabhair ó chomhairleoir dlí na cuideachta.

Beart 7 Comhoibriú a lorg

Trí Fhardal ENISA a úsáid go tapa, rinneadh roinnt CSIRT-anna sa tír chéanna a aimsiú agus rinneadh teagmháil leo. Socraíodh cuairt láithreáin le ceann amháin acu don cheannaire foirne a bhíodhas tar éis a earcú. D’fhoghlaim sé faoi ghníomhaíochtaí náisiúnta CSIRT agus d’fhreastail sé ar chruinniú.

Bhí an cruinniú sin thar a bheith cuiditheach maidir le samplaí a bhailiú de mhodhanna oibre agus maidir le tacaíocht a fháil ó chúpla foireann eile.

Beart 8 An Plean Gnó a Chur Chun Cinn

Déantar cinneadh chun fórais agus figiúirí a bhailiú ó stair na cuideachta. Tá se sin thar a bheith úsáideach i dtaca le forléargas staitisticiúil ar an staid slándála IT. Is ceart leanúint den bhailiú sin nuair atá an CSIRT faoi lánseo d’fhonn na staitisticí a choimeád cothrom le dáta.

Rinneadh teagmháil le CSIRT-anna náisiúnta eile agus rinneadh agallaimh leo faoina gcuid cásanna gnó. Rinne siad tacaíocht a sholáthar trí roinnt sleamhnán a thiomsú ina raibh faisnéis faoi forbairtí le déanaí maidir le teagmhais slándála IT agus faoi chostais teagmhas.

Sa chás samplach seo de CSIRT Samhailteach, ní raibh aon ghá mór lena áiteamh ar an lucht bainistíochta cé chomh tábhachtach ata gnó IT, agus, dá bhrí sin, ní raibh sé deacair ceadú a fháil don chéad chéim. Rinneadh cás gnó agus plean tionscadail a ullmhú, lena n-áirítear meastachán ar na costais tosaithe agus costas na hoibríochta.

Beart 9 Sreabhadh próisis agus nósanna imeachta oibríochta agus teicniúla a bhunú

Díríonn CSIRT samhailteach ar sheirbhísí lárnacha a sholáthar:

- Foláirimh agus Rabhaidh
- Fógairtí
- Láimhseáil Teagmhas

D'fhorbair an fhoireann nósanna imeachta a oibríonn go maith agus atá sothuigte ag gach ball foirne. D'earcaigh an CSIRT samhailteach saineolaí dlí freisin chun déileáil le dliteanais agus leis an bpolasaí maidir le slándáil fhaisnéise. Ghlac an fhoireann roinnt uirlisí úsáideacha agus d'aimsigh siad faisnéis chuiditheach faoi shaincheisteanna oibríochta trí phlé a dhéanamh le CSIRT-anna eile.

Gineadh teimpléad seasta le haghaidh ábhar comhairleach maidir le slándáil agus le haghaidh tuairiscí faoi theagmhais. Úsáideann an fhoireann RTIR chun teagmhais a láimhseáil.

Beart 10 An fhoireann a oiliúint

Déanann an CSIRT samhailteach cinneadh chun gach duine dá fhoireann theicniúil a chur ar an gcéad chúrsa TRANSITS eile atá ar fáil. Ina theannta sin, freastalaíonn ceannaire na foirne cúrsa CERT/CC dar teideal Managing a CSIRT.-----

Beart 11: Ceacht a dhéanamh

Le linn chéad seachtainí na n-oibríochtaí, úsáideann an CSIRT samhailteach roinnt cásanna samhailteacha (a fuarthas mar shamplaí ó CSIRT-anna eile) a úsáideadh mar cheacht. Ina theannta sin, d'eisigh siad ábhar áirithe comhairleach a bhí bunaithe ar fhíorfaisnéis leochaileachta arna dáileadh ag díoltóirí crua-earraí agus bogearraí ar ábhar é a athraíodh agus a oiriúnaíodh de réir riachtanais na cliantachta.

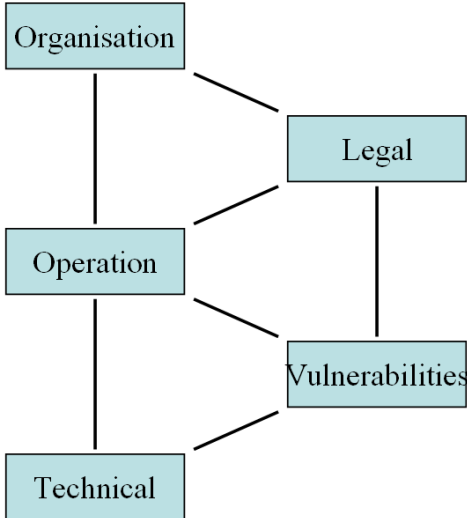
A.4 Ábhar Samplach as Cúrsaí CSIRT

TRANSITS (Le caoinchead ó Terena, <http://www.terena.nl>)

Course structure



- Five modules
- Independent, but linked
- 12-14 hours work in 2 days
- Practical exercises include
 - Analyse incidents
 - Organisational plan
 - Incident response plan



```
graph TD; Organisation --> Operation; Operation --> Technical; Operation --> Legal; Operation --> Vulnerabilities; Legal --> Vulnerabilities;
```

CSIRT training course

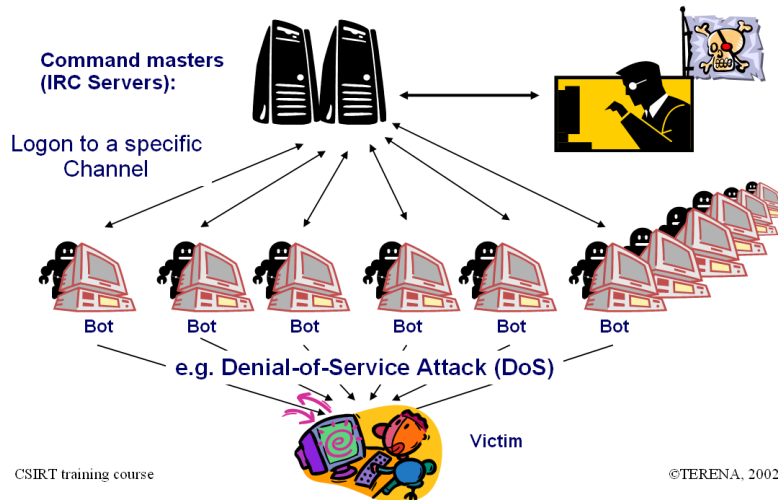
©TERENA, 2002-6

◀ ▶ ↺ ↻

Forléargas: Struchtúr an chúrsa

Malicious Code

Malicious IRC Bots - A botnet in action

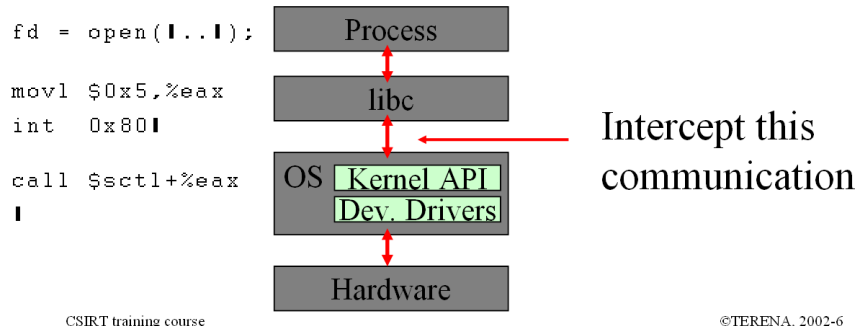
As an *Modúl Teicniúil*: Cur Síos ar Botnet

Malicious Code

Rootkits - Basic design



- Replacing binaries is easily detected (tripwire et al).
- A more elegant approach would deliver false data to **all** processes -> Modify kernel



As an *Modúl Teicniúil*: Bundeardh Fréamhthrealaimh

Who is the Biggest Threat?

Employees?

- Secure h/w & s/w?
- Firewalls?
- Anti-virus s/w?



Customers/Students?

Viruses/Worms

LoveBug, CodeRed, Nimda, Slammer, ...

Cost \$1T worldwide

Need user help to spread:

- Unexpected attachments
- Unneeded programs
- Unwary users get caught

Suppliers/Partners?

Do you know?

DTI* data indicates:

- 68% suffered a malicious incident
- Two thirds have no info security policy
- 57% have no contingency plan for incidents



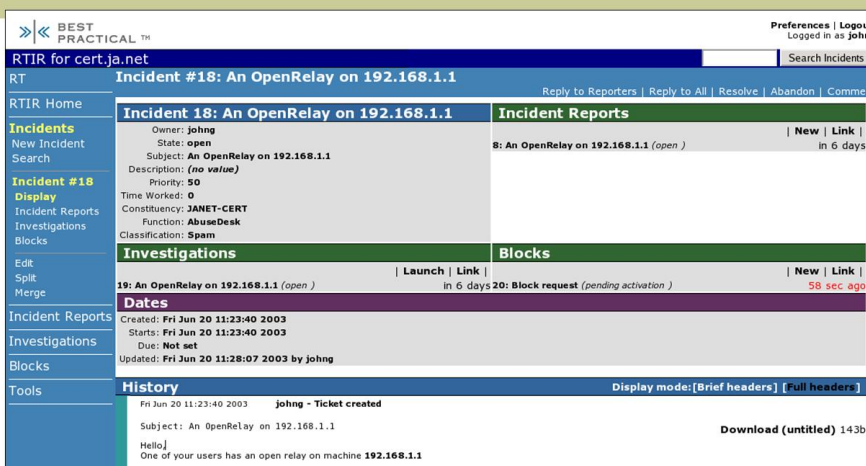
CSIRT training course

* UK Department for Trade & Industry Information Security Breaches survey 2004

©TERENA, 2002-6

As an *Modúl Eagrúcháin*: Laistigh nó Lasmuigh – cá bhfuil an bhagairt is mó?

e.g. RTIR incident page



CSIRT training course

©TERENA, 2002-6

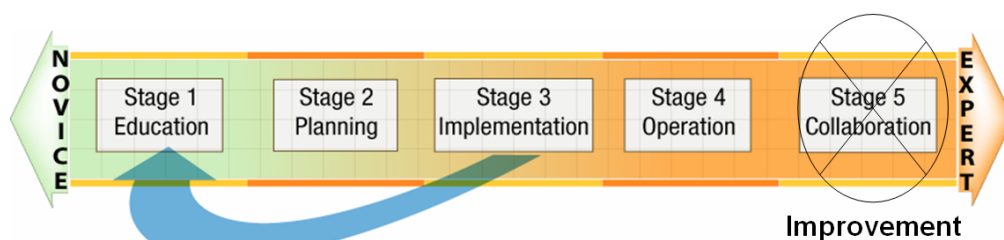
As an *Sliocht Oibríochta*: Iarraidh ar Rianaire maidir le Freagairt Teagmhas (RTIR)

“Setting up of CSIRTs” (le caoinchead ó CERT/CC, <http://www.cert.org>)

Gabhann ENISA buíochas le Foireann Forbartha CSIRT sa Chlár CERT as cead a thabhairt ábhar as a gcúrsaí oiliúna a úsáid!

Stages of CSIRT Development

- Stage 1 Educating the organization
- Stage 2 Planning effort
- Stage 3 Initial implementation
- Stage 4 Operational phase
- Stage 5 ~~Peer collaboration~~ — Improvement of the CSIRT



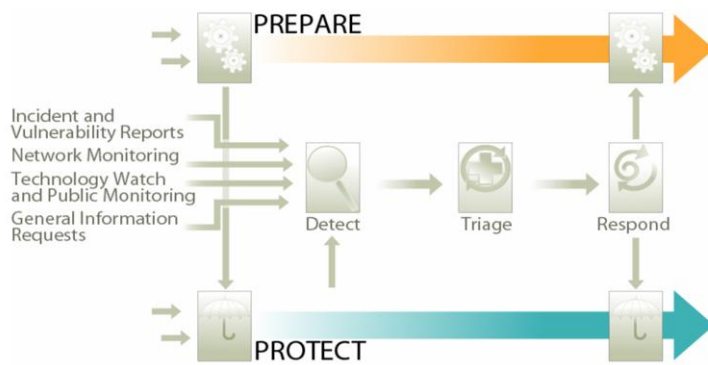
© 2006 Carnegie Mellon University

2



As Cúrsa Oiliúna CERT/CC: Céimeanna i bhforbairt CSIRT

Incident Management Best Practice Model



© 2006 Carnegie Mellon University

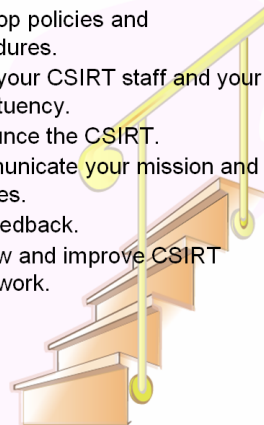
3



As Cúrsa Oiliúna CERT/CC: Dea-chleachtas i dtaca le bainistiú teagmhas

Basic Implementation Steps

- Gather information.
- Identify the CSIRT constituency.
- Determine the CSIRT mission.
- Secure funding for CSIRT operations.
- Determine CSIRT range and levels of service.
- Determine CSIRT reporting structure, authority and organizational model.
- Identify interactions with key parts of the constituency.
- Define roles and responsibilities for interactions.
- Create a plan, obtain feedback on the plan.
- Identify and procure personnel, equipment and infrastructure resources.
- Develop policies and procedures.
- Train your CSIRT staff and your constituency.
- Announce the CSIRT.
- Communicate your mission and services.
- Get feedback.
- Review and improve CSIRT framework.



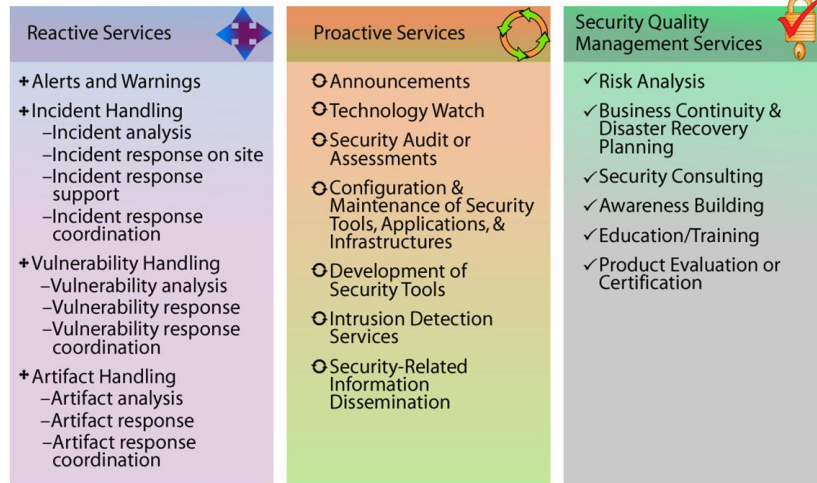
© 2006 Carnegie Mellon University

4



As Cúrsa Oiliúna CERT/C: Na bearta atá le déanamh le linn CSIRT a chur ar bun

Range of CSIRT Services



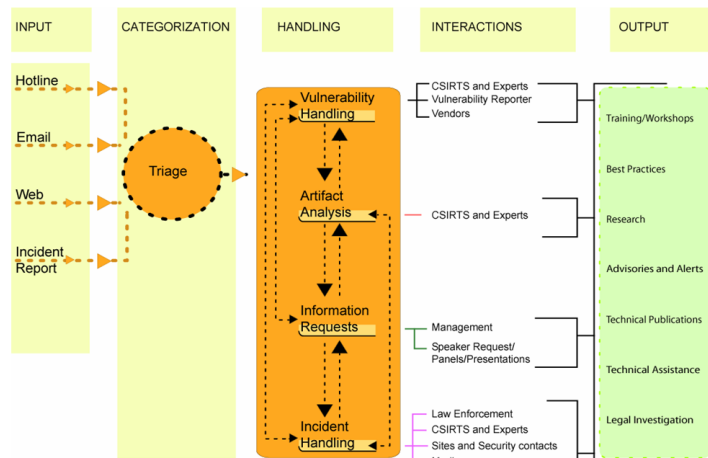
© 2006 Carnegie Mellon University

5



As Cúrsa Oiliúna CERT/CC: Na seirbhísí atá CSIRT in ann a sholáthar

Service Integration



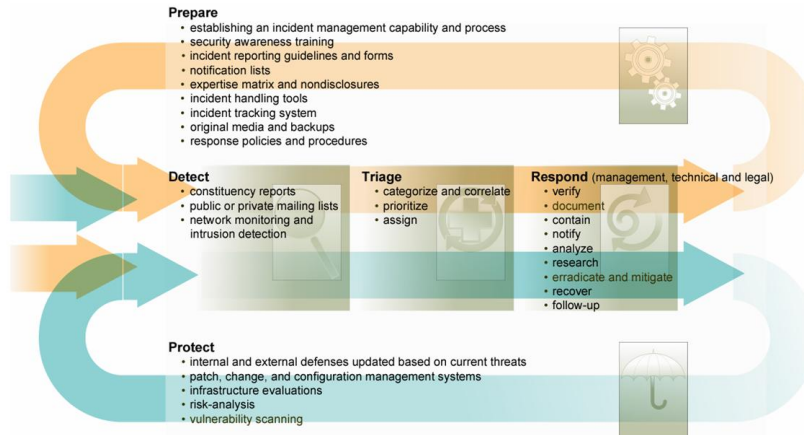
© 2006 Carnegie Mellon University

6



As Cúrsa Oiliúna CERT/CC: An sreabhadh oibre maidir le bainistiú teagmhas

Incident Response Starts Before an Incident Occurs



© 2006 Carnegie Mellon University

8

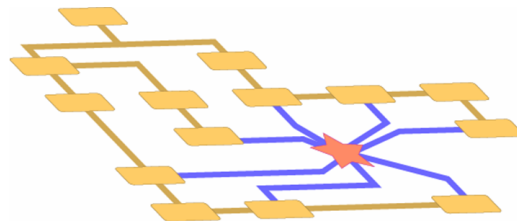


As Cúrsa Oiliúna CERT/CC: Freagairt teagmhais

Organizational Models

When designing the vision of your CSIRT, you need to think about how the CSIRT will operate and interact with the organization and constituency.

You need to envision a model that can be implemented.

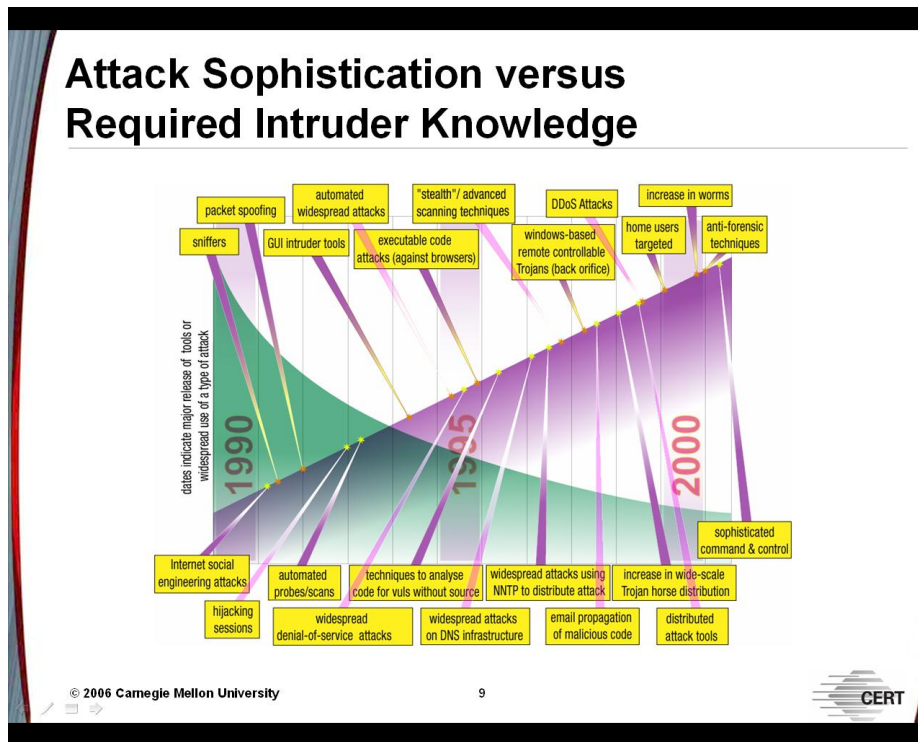


© 2006 Carnegie Mellon University

7



As Cúrsa Oiliúna CERT/CC: Conas a eagrófar an CSIRT?



As Cúrsa Oiliúna CERT/CC: Easpa eolais is cúis le tuilleadh damáiste